

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF WISCONSIN
GREEN BAY DIVISION

UNITED STATES OF AMERICA,)
)
Plaintiff,) Case No. CR 18-157
) Green Bay, Wisconsin
vs.)
) August 14, 2019
THOMAS J. OWENS,) 1:35 p.m.
)
Defendant.)

TRANSCRIPT OF EVIDENTIARY HEARING
BEFORE THE HONORABLE WILLIAM C. GRIESBACH
UNITED STATES CHIEF DISTRICT JUDGE

APPEARANCES:

For the Plaintiff

UNITED STATES OF AMERICA:

United States Dept of Justice
(ED-WI)
By: DANIEL R. HUMBLE
Office of the US Attorney - 205
Doty St - Ste 301
Green Bay, WI 54301
Ph: 920-884-1066
Fax: 920-884-2997
Daniel.Humble@usdoj.gov

For the Defendant

THOMAS J. OWENS:
(Present)

Pruhs & Donovan SC
By: CHRISTOPHER D. DONOVAN
757 N Broadway - Ste 401
Milwaukee, WI 53202
Ph: 414-221-1950
Fax: 414-221-1959
donovanc34@hotmail.com

U.S. Official Transcriber:
Transcript Orders:

JOHN T. SCHINDHELM, RMR, CRR,
WWW.JOHNSCHINDHELM.COM

Proceedings recorded by electronic recording,
transcript produced by computer aided transcription.



TRANSCRIPT OF PROCEEDINGS

Transcribed From Audio Recording

* * *

THE CLERK: The Court calls Case 18-CR-157, United States of America vs. Thomas J. Owens for an evidentiary hearing. May I have the appearances, please?

MR. HUMBLE: Dan Humble for the Government, along with Misha Linsmayer (phonetic) from our office, Your Honor.

THE COURT: Good afternoon.

MR. DONOVAN: Attorney Chris Donovan appearing on behalf of Mr. Owens who is here in person on my right. And then, also to my immediate right is our expert, Peyton Engel.

THE COURT: Okay. Good afternoon.

So we have put this on for a hearing on the motion to disclose investigative BitTorrent software and related documents. And the government has opposed the motion on the basis of the law enforcement privilege?

MR. HUMBLE: Yes, Your Honor.

THE COURT: Or investigation privilege?

And so the -- I guess, what do you -- Mr. Donovan, it's your motion, how would you plan on proceeding?

MR. DONOVAN: Your Honor, what I envision is I would call my expert. I think that we have at least the initial burden under Rule 16 to show that the requested material is material to preparing our defense.

1 THE COURT: Uh-huh.

2 MR. DONOVAN: And then I think the burden on the law
3 enforcement privilege would fall to the government, so they can,
4 you know, carry that burden when they call their witness.

01:46 5 THE COURT: That sounds good. Go ahead. You may call
6 your witness.

7 MR. DONOVAN: Do you want him up on the witness stand?

8 THE COURT: Oh, yeah.

9 MR. DONOVAN: Okay.

01:46 10 THE CLERK: Please raise your right hand.

11 Do you solemnly swear the testimony you are about to
12 give today is the truth, the whole truth and nothing but the
13 truth so help you God?

14 THE WITNESS: I do.

01:46 15 THE CLERK: Please state and spell your first and last
16 name for the record.

17 THE WITNESS: My name is Peyton Engel, that's
18 P-e-y-t-o-n, E-n-g-e-l.

19 THE COURT: Thank you, Mr. Engel.

01:48 20 Go ahead, Mr. Donovan, you may proceed.

21 MR. DONOVAN: Thank you, Your Honor.

22 PEYTON ENGEL, DEFENSE WITNESS, DULY SWORN

23 DIRECT EXAMINATION

24 BY MR. DONOVAN:

01:48 25 Q. Good afternoon, Mr. Engel. I just want to run through a few

1 background questions with you. Can you state your education
2 background?

3 A. I have a bachelor's degree in Russian from Grinnell College,
4 a master's in Russian literature from the University of
01:53 5 Wisconsin-Madison, and a JD from the University of
6 Wisconsin-Madison.

7 Q. And can you do a brief overview of your work history?

8 A. Yes. In about 1997, I went into the field of IT networking,
9 the bottom having fallen out of the Russian literature market.
01:53 10 And I specialized in computer security for about 16 years. And
11 that included doing forensic investigations and incident
12 response.

13 Q. And where do you work now?

14 A. I currently work for a law firm in Madison, Wisconsin that's
01:54 15 called Hurley Burish.

16 Q. And can you just give a brief on overview, not necessarily
17 maybe listing everything, but some examples of your
18 certifications and continuing education in the computer field.

19 A. I routinely provide training. So I speak at conferences and
01:58 20 at trainings, for example, for the state public defender, mostly
21 regarding how to work with computer experts, how litigators
22 should work with computer experts.

23 I maintain the CISSP -- that's Certified
24 Information -- CISSP, Certified Information Systems Security
01:58 25 Professional certification -- which is sort of a broad or a

1 generalist security certification but it's, for better or worse,
2 one of the standard ones that people obtain in the field. It
3 includes some requirements for forensics and incident response
4 knowledge as well.

01:59 5 Q. Thank you. You mentioned that you train other professionals
6 in this area, correct?

7 A. Yes.

8 Q. And so you've spoken at different conferences?

9 A. Yes.

01:59 10 Q. And do you also have some published works?

11 A. Yes.

12 Q. Can you give an example of a few of those?

13 A. The most recent one was an article on cell phone forensics
14 and that appeared in The Champion, which is the National
01:59 15 Association of Criminal Defense Lawyers publication.

16 Q. And you've testified in court before?

17 A. Yes.

18 Q. And related to, again, computer issues?

19 A. Yes. I've appeared as an expert witness. This is my first
02:06 20 venture into federal court, but I've appeared as an expert at
21 trial and at evidentiary hearings in a number of state court
22 proceedings.

23 Q. Can you give a rough estimate?

24 A. My affidavit actually lists some specific ones. I've
02:06 25 probably appeared in 10 or so, 10 or 12. And then I've been an

1 expert in dozens more, but those haven't gone to trial.

2 Q. Okay, thank you. Okay. Have you also done some prior work
3 for law enforcement before?

4 A. Once in a while. The most notable incident was -- well,
02:07 5 never been deputized or anything like that, but in the course of
6 my work I've assisted -- the FBI was the most notable, in an
7 industrial espionage case down in Madison.

8 Q. So is it fair to say you've worked on both the defense side
9 and law enforcement?

02:08 10 A. Yes, though heavily more on the defense side.

11 Q. Correct. Okay. Okay. Can you kind of explain what a
12 peer-to-peer network is and how it operates?

13 A. Sure. A peer-to-peer -- well, the standard architecture on
14 the internet is what's called a client server architecture. You
02:09 15 have a centralized resource, say a website or something like
16 that, that many people want to access. And so they'll use a
17 client piece of software like a web browser to see the web
18 server. And that shares this one central resource among many
19 other users.

02:09 20 A peer-to-peer architecture is just a different
21 arrangement. Instead of having one central resource, resources
22 are distributed across the network and users share and consume
23 on an as-needed basis.

24 Q. And to access a peer-to-peer network you have to download
02:09 25 like a special type of software?

1 A. Yes. There's usually a peer-to-peer client software
2 involved.

3 Q. Can you explain what open source software would be versus
4 not open source?

02:10 5 A. Sure. Software is developed by programmers. And
6 programmers write in a computer language. So, for example, C or
7 Java. And that language is compiled -- the C or Java code
8 itself is not what the computer runs. It's compiled and
9 generated into an executable program for the computer. But that
02:11 10 code that the programmers write is called the source code.

11 Closed source software means it's not publicly
12 accessible. Open source software means that the source code is
13 available for others to review or potentially update and modify.

14 Q. So would most of these peer-to-peer programs be open source
02:13 15 software?

16 A. There's a variety. There are -- so, for example, at issue
17 in this case is BitTorrent. There are both open and closed
18 source BitTorrent clients.

19 Q. Okay. Now, is it your experience and knowledge that all
02:14 20 software is subject to having bugs or errors or malfunctions in
21 it?

22 A. Yes. This is a universal truth. I mean, not all software
23 has tons of bugs. Some is sounder than others. But sort of the
24 gold standard for software bug-trimming would be avionics
02:16 25 software. And we've just recently seen the 737 Max disasters.

1 So it's a certainly heavily reviewed, heavily audited code that
2 didn't function as expected.

02:16

3 Q. So even commercial products like Microsoft Word or Excel or
4 other, you know, highly common programs have bugs and errors,
5 correct?

02:20

6 A. Yes. And these are systems that are wildly deployed, you
7 know, used by many, and there's a robust system for reporting
8 issues and, you know, having them escalated and filtered through
9 technical support. But I still get updates from Microsoft
10 probably twice a month.

11 Q. Can you explain a little bit more about like how they're
12 addressed? So, for example, is there things called "patches"
13 that fix errors?

02:20

14 A. Right. A "patch" is a term for usually a small update to a
15 piece of software. So there are patches. And then larger
16 things might be called "service packs." These are basically
17 usually small executable pieces of code that are delivered and
18 they update some aspect of a piece of software that's been
19 deployed out in the field.

02:21

20 Q. Now, do most programs also go through what's called "beta
21 testing"?

22 A. Yes. Generally there's a beta phase before it's sent into
23 full production.

24 Q. Could you explain what a beta test would be?

02:21

25 A. Sure. So a beta testing happens when people think the

1 software is pretty much done and more or less ready to deploy.
2 They'll deploy it in a way that generally more sophisticated
3 users who would be good at spotting issues and good at reporting
4 the issues, have a chance to tinker with the software and to use
02:24 5 it and get the hang of it before it gets a general release.

6 Q. Is it kind of fair to say they kind of put it through its
7 paces before it becomes generally used?

8 A. That's the idea of beta testing.

9 Q. And just to be clear, are most beta testers outside the
02:25 10 entity or the company that made the software?

11 A. That depends on the kind of software and who the eventual
12 user base is. Probably in the world at large, yes, but for any
13 given project it might be different.

14 Q. Now, can you describe briefly what the interface would look
02:25 15 like on a peer-to-peer program?

16 A. Well, it's usually a graphical user interface these days.
17 There's a way of searching for -- let's restrict ourselves to
18 peer-to-peer file sharing programs. There are other things out
19 there, but there would be an interface for searching for the
02:26 20 type of file you want to find.

21 So, for example, if I want to download the latest Star
22 Wars movie or something like that, there would be a place to
23 type in what I'm searching for and a place to see results and
24 select which ones I wanted to obtain.

02:26 25 Q. So there would be like a search bar that you could type in

1 like a text search, for example?

2 A. Yeah. I mean, something -- something like that is present
3 somewhere along the way. Different clients will look different,
4 but, yes, that functionality is there in one form or another.

02:27 5 Q. Can users also search by hash values if they would know the
6 hash value of the particular file that they want?

7 A. It would be strange for a user to even understand what a
8 hash value is. I have no -- I mean, there's no reason the
9 software couldn't support that, but for someone to sit and enter
02:27 10 a 48-digit hexadecimal numbers -- I wouldn't think most users
11 would do that.

12 Q. And maybe just to make sure everyone's on the same page, can
13 you briefly explain what a hash value is?

14 A. Right. So a hash value, sometimes people call it the
02:28 15 "digital fingerprint" of a file. So suppose you have two files
16 and you want to know if they're the same. Rather than go and
17 bit-by-bit compare them, you can pass them each through a
18 certain kind of mathematical function, called a "hash function,"
19 and you obtain a number. And if those two numbers are the same,
02:28 20 then the chances are astronomically small that the two files are
21 different. And so a hash value is sort of a shorthand for
22 identifying a file or a piece of a file.

23 Q. Now, you've reviewed the pleadings in this case, correct?

24 A. Yes. At least the initial ones.

02:29 25 Q. Including the government's response brief --

1 A. Yes.

2 Q. -- to our motion to compel?

3 Now, they raise this concern about if the program's
4 turned over that, you know, hash tags could be manipulated to
02:30 5 change and then they'd be harder to detect. Right? Do you
6 remember -- do you recall that?

7 A. I do recall that.

8 Q. Okay. Now, why in your opinion would that be a red-herring
9 argument?

02:30 10 A. For a couple of reasons. First, I presume, but do not know,
11 that the database of known hash values is separate from the
12 program itself. So one could look at the program without
13 necessarily seeing the full list of things that it looks for.

14 Second, the government discloses hash values every
02:31 15 time it applies for a search warrant. You see not only the hash
16 value of the file that they say they've obtained, but also the
17 file name that is associated with it. So it's not that any
18 individual hash value is that big a secret.

19 Third, it's possible for anyone on the internet to go
02:31 20 ahead and change a single bit in a file today without the
21 software having been disclosed. And that would change the hash
22 value and it would no longer trigger the automated alerts that
23 the Torrential Downpour software generates.

24 That's something that could happen today for free and
02:33 25 without any -- you know, without any need for knowledge of the

1 code base.

2 But fourth, that would actually reduce the ability to
3 share or at least the ease with which people are sharing
4 contraband materials on the internet because of all the hash
02:33 5 value changes -- values change. Then the Torrent clients won't
6 know how to find the software for the images or movies or
7 whatever it is they're downloading anymore because the whole
8 thing is premised on a shared, you know, set of hash values.

9 So, yes, that could happen. But it doesn't seem to me
02:34 10 to be either a realistic possibility or one that would -- I
11 mean, it would actually probably cut down on the sharing of
12 child pornography on the internet.

13 Q. Now, you talked earlier about source code versus the program
14 itself, right?

02:34 15 A. Yes.

16 Q. Can you explain what concerns there might be about turning
17 over source code?

18 A. So the gold standard for understanding how a piece of
19 software works is to review the source code. You get to see
02:34 20 pretty much everything it's capable of. And you can then see
21 all of the inputs that it takes and all of the ways in which it
22 gives output and all of the logic that it operates on. So the
23 concern there would be that by knowing that, one would know
24 something that couldn't otherwise be known.

02:36 25 So, for example, from time to time, and I believe in

1 this case, the government raises the concern that this kind of
2 disclosure would impede future or ongoing investigations. So I
3 can think of a couple ways that that might happen.

4 One is, that we know from reading the warrants here
02:37 5 and in other cases, that RoundUp pretends to be sharing files in
6 order not to get kicked off the network or throttled from being
7 able to download files.

8 If it were the case that RoundUp always shared the
9 same list of files, that might be a way of recognizing RoundUp
02:39 10 and people who wanted to avoid being tagged by it would simply
11 hang up the phone whenever something sharing those files
12 connected.

13 Another thing might be that -- and this is
14 hypothetical. I don't know this because I haven't had access to
02:40 15 the source code. But another thing might be that if the system
16 is designed so that -- to prevent law enforcement in one
17 jurisdiction from accidentally investigating other users of
18 RoundUp in another jurisdiction, maybe there's something about
19 the way that it establishes its connection or operates -- or
02:41 20 interacts with the systems it's investigating that could be
21 recognized. That would be another sort of handshake signature
22 that you could figure out this is RoundUp connecting to me and
23 then hang up the phone again.

24 That would be -- those would be two ways that I can
02:41 25 think of that would be potentially problematic.

1 Q. Now, those concerns wouldn't be raised if it was just
2 getting access to the program and not the source code, correct?

3 A. Well, it would be less of a concern. It would sort of
4 depend on how the program operates and what we'd be able to
02:43 5 observe about it.

6 Q. Fair enough. I understand, again, you obviously don't have
7 access to the program so you can't say for sure.

8 Okay. And I just want to clarify one thing. When you
9 say RoundUp, you're using that interchangeably with Torrential
02:43 10 Downpour?

11 A. Yes. I am sorry. That's a habit that I have. The
12 investigative software, which is RoundUp-like, which is used on
13 BitTorrent, is called "Torrential Downpour" from what I've read.

14 Q. Okay. So going back to peer-to-peer network I guess
02:44 15 architecture. So it's a decentralized network, correct?

16 A. Yes.

17 Q. And this would be to allow sharing more efficiently and
18 faster than if it was just in a centralized network?

19 A. Right. So the problem that the designers were attempting to
02:45 20 solve was, how do we exchange large files that aren't hosted at
21 some giant file repository like a Google Docs or something like
22 that? How do we just trade large files on the internet?

23 And the issue is that when we purchase a connection to
24 the internet from our internet service provider, whether it's
02:46 25 AT&T or Comcast or whatever it is, the connection we get is

1 generally what's called asymmetrical. Meaning that we can
2 download things much faster than we can upload them. Because
3 the people who provision those circuits realize correctly that
4 for most people's purposes that's the right way to do it. Most
02:46 5 people are much more interested in downloading things than they
6 are in uploading things.

7 So you might get, say, from a Spectrum, Charter
8 Spectrum account you might get 200 megabits downstream to your
9 house so can watch Netflix on several TVs at once, but you might
02:46 10 only get, you know, 30 or 50 megabits upstream. So the problem
11 is if -- let's say you and I want to exchange a file -- well, I
12 want to get a file from you. I'm limited. Even though I can
13 download things with blazing speed, I'm limited to getting the
14 file by the fastest speed that you can upload. And so that
02:49 15 makes things crawl to a halt, and it also means you can't be
16 sharing multiple files at once, et cetera.

17 So the insight of BitTorrent is, hey, why don't we
18 chop the files up. Why don't we have the files stored on
19 multiple systems around the internet, or at least realize that
02:49 20 they are stored in multiple systems around the internet, chop
21 them up into segments, and I can grab one segment from system A,
22 one segment from system B, one segment from system C, and then
23 get the benefit of my fast bandwidth by being able to download
24 from several sources at once and you get the file faster that
02:50 25 way.

1 Q. Can you describe briefly how computers connect to the
2 internet and maybe also discuss what an IP address is?

3 A. Sure. So one of the hard problems in computing in the '70s
4 was how do we get computers to talk to each other. And what
02:51 5 came out of this, the sort of system that emerged and towers
6 above all others today is what's called the "internet protocol."
7 It's a series of rules or standards by which one communicates on
8 the internet.

9 And one of the challenges that it solves is how do we
02:52 10 route a message. So let's say we have a network that spans the
11 nation or even the world, how do I get a message from one
12 computer to another?

13 And so the way this is accomplished is via IP
14 addresses and routing protocols. But for the purposes of this
02:53 15 conversation, every machine that is connected to the internet is
16 assigned or associated with at least one IP address.

17 And when we are -- you can think of -- as the machine
18 sends messages across the internet, you can think of this as
19 being like the send and return addresses on a mail envelope. It
02:53 20 has a "destination" IP address, each message does, and a "sent
21 from" IP address. And so that when the guy at the other end of
22 the connection gets the message, he knows where to reply to.

23 So IP addresses are distributed more or less
24 geographically. So we can -- by IP address, we can draw some
02:54 25 inferences about where a system is located in the physical world

1 and which internet service provider allocates it. And this is
2 what allows investigators, when they find an IP address that
3 they think is associated with a crime, they can get an
4 administrative subpoena or some other mechanism that compels the
02:54 5 relevant internet service provider to disclose the identity of
6 the subscriber who was using that IP address at the time.

7 Q. Okay. So I'd like to talk a little bit about how
8 BitTorrent's a little different than maybe perhaps other
9 peer-to-peer programs. So you've talked about these little
02:55 10 pieces of a file. Would those be called "torrents"?

11 A. So a torrent -- at least the way I think of it is, there's a
12 thing called a "torrent file" which is kind of like a recipe for
13 obtaining and assembling a given set of contents.

14 So, again, let's use the example of the latest Star
02:56 15 Wars movie. It would list the -- for each segment of the file
16 some directions for where to find that and how to, once you've
17 got all the segments, how to assemble that into the finished
18 product.

19 Q. And then -- so a torrent is basically a map that then helps
02:57 20 the computer receiving these different pieces to assemble them,
21 correct?

22 A. Right. It tells you -- it's kinda like a recipe. It tells
23 you what ingredients to get and how to put them together.

24 Q. Okay. And, again, BitTorrent is decentralized? There's no
02:57 25 central server or hierarchy, correct?

1 A. Yes.

2 Q. Okay. I'd like to talk now about Torrential Downpour, or
3 what you call RoundUp, and how it modifies the normal BitTorrent
4 program. Okay? So first off, Torrential Downpour is not open
02:58 5 source, correct?

6 A. Correct. The source code is secret.

7 Q. So, not publicly available from any other source, right?

8 A. Correct.

9 Q. Do you know anything about I guess the origin or who created
02:58 10 these programs?

11 A. There are publications available, some of them authored by
12 the gentleman at the prosecution table, that describe its
13 creation. It's a collaboration between law enforcement and some
14 computer scientists.

02:59 15 Q. Okay.

16 A. I couldn't name them right off the top of my head.

17 Q. And that's fine. I'm not asking you to name them.

18 There's certain things we do know about Torrential
19 Downpour that is different than the normal BitTorrent program,
02:59 20 correct?

21 A. Yes.

22 Q. Okay. Is one of the differences what's called single source
23 downloading?

24 A. Yes. As I described earlier, the goal of BitTorrent was to
02:59 25 allow people to obtain files in pieces from multiple sources.

1 That was the point of it.

2 For law enforcement purposes, though, in order to
3 prove that a user has the entirety of one file, it's necessary
4 to get all of the segments from that one target computer. So
03:00 5 one of the things that RoundUp is designed to do is obtain an
6 entire download from a single source.

7 So it's speaking the BitTorrent protocol, but doing so
8 in a way that sort of subverts the purpose of it. It's not
9 breaking any rules, but it's definitely doing something out of
03:01 10 the ordinary and deviating from the BitTorrent standard.

11 Q. And again, this isn't something a normal BitTorrent user
12 would do or how it would operate.

13 A. It's not something a normal BitTorrent user would probably
14 want to do, since it just makes things go more slowly. But,
03:01 15 yes, standard BitTorrent software would not be capable of doing
16 this.

17 Q. Now, you mentioned earlier that it also might basically fake
18 file share so it doesn't get throttled down on the network. Can
19 you explain that a little bit more?

03:02 20 A. So one of the things that people quickly discovered when the
21 BitTorrent standard was first developed is that people would do
22 what's called "leaching." They would come and download a bunch
23 of stuff, but they wouldn't be sharing anything. So they would
24 be consuming BitTorrent resources but not contributing back.

03:02 25 So various efforts were made to force people to share

1 at least what they had downloaded, and maybe other things as
2 well, so that they weren't just a drag on the network; so that
3 they're contributing.

4 And so what you see is clients that aren't sharing
03:05 5 anything won't get preferential treatment in terms of downloads.
6 They won't get necessarily access. Their ability to download
7 will be throttled.

8 Q. And why would law enforcement not want to be participating
9 in the sharing?

03:05 10 A. Well, there are a couple of reasons. One would be, they
11 don't want to commit any crimes.

12 The other one -- I mean, that's probably the major
13 one. But they probably also want to appear as though at least
14 from time to time they are sharing contraband because then
03:11 15 they'll get more interesting connections inbound to them.

16 Q. And do you have any I guess speculation on how they could
17 hold themselves out as sharing when they're not, in fact,
18 sharing?

19 A. Oh, you simply respond to search queries saying, yeah, I've
03:11 20 got this or -- you know, I don't know the exact dimensions of
21 the protocol that they're speaking. You know, I don't know
22 exactly what messages they're sending, but they can advertise
23 what they've got.

24 Q. Now, another difference is, does Torrential Downpour run
03:13 25 automatically?

1 A. Yes. We've learned -- well, automatically. Presumably a
2 user launches it initially. So it's maybe not fully automated.
3 But once it's on, it just sits and runs. It runs around the
4 clock, unattended.

03:13 5 Q. And do we know how that actually is carried out or what
6 means are used to do that, or is that something, again, that you
7 don't know?

8 A. I mean, I presume, without firsthand knowledge, that it just
9 sits in a lab somewhere and runs. It gets set up and launched
03:14 10 like any other process and it's left running and then people
11 check on it from time to time to see what it's found.

12 Q. Okay. Does Torrential Downpour also generate special data
13 logs?

14 A. Yes, it does.

03:14 15 Q. Now, how would we judge the reliability of those logs that's
16 generated by the same program that we don't have access to?

17 A. I -- well, without access I have no objective way of judging
18 the accuracy of the logs.

19 So, for example, I've seen log files and they
03:15 20 oftentimes will describe events that can be verified via other
21 means; for example, in the context of a criminal case.

22 But what we don't know -- there's sort of confirmation
23 bias here. What we don't know is how many log files are
24 generated that don't result in prosecutions, or how many
03:15 25 warrants are executed that don't result -- based on those log

1 files that don't result in prosecutions. We don't have access
2 to that information so there's -- we don't have a way of
3 evaluating whether the system is accurate in general or not.

03:16 4 Q. Does this kind of maybe implicate that you'd have a false
5 positive? Is there -- can you describe what a false positive
6 might be in computer --

7 A. Sure. In testing -- in general, any time you have a test to
8 look for a condition, there are two kinds of errors that you are
9 worried about. One is a false positive result. In other words,
03:16 10 the system, whatever it may be, falsely reports the condition
11 exists. The other one is a false negative. The condition
12 falsely reports -- or, I'm sorry, the test falsely reports that
13 the condition does not exist.

14 And these are things which are tracked very carefully.
03:17 15 For example, in medical testing, you know, you have a test which
16 is 99 percent accurate for finding this kind of cancer. What
17 they mean is there's 1 percent that they're getting either false
18 positives or false negatives and, you know, giving a
19 misdiagnosis potentially on that basis.

03:18 20 So here as well we know of times when the system has
21 given positive alerts, but we only know the ones that resulted
22 in prosecutions. So we don't know the false-positive rate or
23 the false-negative rate of Torrential Downpour.

24 Q. And the logs themselves again don't shed any light on that,
03:18 25 correct?

1 A. Right. They -- they report what the software reported.
2 They're a record of what the software reported.

3 And there's -- the logs themselves, you know, purport
4 to be accurate records of events that the software engaged in,
03:22 5 but we have no way -- or at least I have no way of verifying
6 their accuracy.

7 Other than, I will say, from time to time there are
8 events in a log that can actually be correlated with records of
9 events elsewhere or other sources of information.

03:22 10 Q. Well, let's talk about this case. So, for example, one way
11 that this supposed single-source download could have been
12 verified was that the image that the program said it downloaded
13 was found later on Mr. Owens' computer, correct?

14 A. Correct.

03:23 15 Q. And in this case did that happen?

16 A. There was -- to my recollection there was an image that the
17 Torrential Downpour reported a single source download of and
18 that image was not found on any of the media seized.

19 Q. Is another difference between Torrential Downpour and the
03:24 20 public version of the program is that Torrential Downpour can
21 get information from target computers like, for example, the
22 version that's being run of the program?

23 A. Torrential Downpour is a BitTorrent client in the sense that
24 it speaks the BitTorrent protocol, but it's really a
03:24 25 surveillance tool. It's designed for gathering information to

1 be used in prosecution, and so it makes records of all kinds of
2 information that would be of no interest to the average
3 BitTorrent user: IP addresses, software versions, segments of
4 files and so forth.

03:25 5 All of that information is used to a greater or lesser
6 extent by a BitTorrent client, but it's not exposed to the user.
7 The user has no knowledge of it. The user just says, "ah, my
8 file got here" and is happy with that.

9 So that's -- that's a difference between Torrential
03:25 10 Downpour and other BitTorrent software, is that the other
11 BitTorrent software is designed for transferring files,
12 Torrential Downpour is designed for supporting interdiction.

13 Q. Okay. Is there any other I guess major differences you're
14 aware of that Torrential Downpour might have that the public
03:25 15 program doesn't?

16 A. I don't believe it's an issue in this case, but I have from
17 time to time in warrant applications seen statements to the
18 effect that Torrential Downpour is capable of tagging a target
19 system.

03:30 20 So one of the other problems that can happen is in say
21 a home network there might be multiple devices, tablets, phones,
22 computers, these days thermostats, alarm systems, et cetera,
23 that all use the internet for communications. And so one of the
24 problems is, well, how do we know which of these devices was the
03:31 25 one that was on the BitTorrent network?

1 And so presumably this involves the placement in a log
2 file somewhere of some piece of information that would be
3 uniquely identifying the system as this is the one to which law
4 enforcement connected. But I'm not aware of that being in play
03:31 5 in this case.

6 Q. Would a tag, if it was placed on a target computer, possibly
7 be in a nonshared portion of the target computer?

8 A. It would possibly be there, yes. I don't know the exact
9 mechanism of tagging. But like I said, I assume it's probably
03:31 10 in a log file somewhere.

11 Q. And again, without access to the program it's impossible to
12 say.

13 A. A tag might be discernible, but, yes, it would be much
14 easier to figure it out if we had access to the program.

03:32 15 Q. Okay. Okay. So, now, in this case you were hired by me,
16 correct?

17 A. Correct.

18 Q. And you reviewed all the digital evidence that was made
19 available by law enforcement.

03:32 20 A. Yes.

21 Q. And so did that include a mirror-image of the computer hard
22 drive --

23 A. Yes.

24 Q. -- that was seized from the search warrant?

03:32 25 A. It did.

1 Q. And also was there several thumb drives?

2 A. Yes.

3 Q. Okay. And again, you also reviewed I think you said the
4 pleadings, like the indictment?

03:33 5 A. Yes.

6 Q. And also the police reports.

7 A. Yes.

8 Q. And the search warrant, correct?

9 A. Yes.

03:33 10 Q. Okay. Now, after you reviewed all of this material did you
11 have several questions that caused you concern?

12 A. One that I recall was that at least some of the single
13 source downloads seemed to happen quite quickly. It's not rare
14 to see single source downloads or logs of single source
03:34 15 downloads -- I've never seen the single source download
16 itself -- but Torrential Downpour logs that describe single
17 downloads that take hours, or even maybe span more than a day.

18 Here at least some of them -- and I don't recall the
19 exact timeframes without refreshing my recollection, but some of
03:36 20 them were quite quick, on the order of less than a minute or
21 maybe even seconds.

22 Q. And why would that be unusual?

23 A. Well, again, the nature of the single source download is
24 that because you're downloading from a single source, you are
03:39 25 subject to whatever the upstream bandwidth limitations of that

1 source are. So that's why it sometimes takes a while to get
2 files, because you're pulling it from a system that's only
3 uploading very efficiently. It's maybe not the only consumer of
4 that upstream bandwidth and, in any case, it's limited by that
03:40 5 pipe size.

6 Q. Was another one of your concerns about what the search
7 warrant meant when it said that law enforcement's investigative
8 focus was directed to Mr. Owens' IP address?

9 A. Right. So search warrant applications derived from
03:40 10 Torrential Downpour information are generally worded pretty
11 obliquely, I assume in order to avoid divulging sensitive
12 information about the software.

13 So I don't have any idea what it means to turn one's
14 investigative focus, what actions that implies. I mean,
03:42 15 presumably at any point in an investigation one's focus is
16 somewhere, but I don't know what it means to turn one's
17 investigative focus towards a certain IP address. I mean,
18 obviously it means I've seen an alert and so I'm taking an
19 interest in the IP address, but I don't know what actions the
03:42 20 investigator takes.

21 I also don't know concretely, you know, in technical
22 terms what it means to be associated with a certain hash value.
23 That would be another -- you know, we just don't know precisely
24 what it is that Torrential Downpour is basing its alerts on. We
03:43 25 know the kind of stuff it is, but not exactly what.

1 Q. And, again, to be clear, this could have been the program by
2 itself running automated that, you know, focused its
3 investigation or, you know, thought that this target computer
4 was associated with a torrent, not necessarily a person sitting
03:43 5 there looking over it, correct?

6 A. Yeah. Based on what I have read in this case and in others,
7 I think it's rare for someone to just sit there watching
8 Torrential Downpour. What happens is they get a bunch of --
9 they come back in the morning, probably see a bunch of log files
03:44 10 and then start digging on those.

11 Q. So in a sense, as far as the actual transactions that occur
12 between Torrential Downpour and the remote client or the target
13 computer, would it be fair to say that really the program's the
14 only witness to what happened at that point.

03:44 15 A. Yeah, I think that's a good analogy. The process of
16 identifying IP addresses in the language of the warrant
17 associated with a piece of contraband and conducting the single
18 source download is probably entirely automated and, you know,
19 was done unattended by a human.

03:45 20 Q. Could the term "associated with a torrent" just means that
21 the target computer says, hey, I have this torrent or this map
22 to a file and not necessarily the file itself?

23 A. I assume it means either I have it or I want it, and I don't
24 know for sure which.

03:46 25 Q. But, again, could it be that it doesn't necessarily have the

1 file; it's just saying that it has the information or the
2 request for the file?

3 A. Oh, certainly. It might even be a false statement.

4 It's possible to imagine that someone, for example,
03:46 5 Torrential Downpour might untruthfully advertise what they have.

6 Q. Okay. Did you also have concerns when the search warrant
7 said that Mr. Owens' computer connected to law enforcement's
8 computer and what that might mean?

9 A. Yeah, I would be curious to know exactly what that means and
03:47 10 what caused it to do so.

11 Q. Okay.

12 MR. DONOVAN: And, Judge, I'm getting towards the end
13 of my questions for Mr. Engel.

14 BY MR. DONOVAN:

03:47 15 Q. So I guess I'd like to kinda conclude with, you know, why
16 you feel you need access to Torrential Downpour to answer all
17 these questions or to answer some of these concerns in the case.

18 So would it be fair to say that you need access to the
19 program to confirm whether Torrential Downpour actually
03:49 20 conducted a single source download the way that it says it does?

21 A. Right. I don't think -- I mean, the time of that particular
22 single source download has come and gone. But I don't have any
23 way to verify how reliably Torrential Downpour conducts single
24 source downloads. So that would be one of the things that I
03:49 25 would want to observe is sort of, in a controlled environment,

1 does it reliably get all of a file from a single source when it
2 reports that it's doing so.

3 Q. And this would be important because whether or not the
4 entire file came from Mr. Owens' computer versus from multiple
03:50 5 computers, would obviously bear on his intent or his knowledge
6 of what occurred, correct?

7 A. I don't know so much knowledge as just actual possession.
8 If someone has a piece of a file, that's different from having
9 the whole file.

03:50 10 Q. And, again, that's, again, also maybe different from having
11 just the torrent for the file.

12 A. Correct.

13 Q. Okay. Because, again, normal peer-to-peer protocol would be
14 a download from multiple sources, not just one. So that would
03:51 15 be pretty crucial to try to figure out.

16 A. Right. So presumably the authors of Torrential Downpour
17 overrode that default behavior of the BitTorrent software. And
18 the question is, did they do a perfect job of that or not.

19 Q. Okay. Are you also interested in knowing what network
03:51 20 traffic is monitored to identify potential target computers?

21 A. Yes. I would be interested to know the specific sorts of
22 messages that Torrential Downpour inspects.

23 We know that it discriminates between network messages
24 that involve hash values that are related to contraband. In
03:52 25 order to do that, it's gotta be looking at the pool of messages

1 in general and then it alerts on the ones that are presumably --
2 their hash values are in a database of known bad files.

3 But, so it's -- effectively it's looking at all of the
4 traffic and then discriminating. It's only alerting on some of
03:52 5 it.

6 Q. So correct me if I'm wrong, but it sounds like it could be
7 doing like a dragnet search of all traffic across a peer-to-peer
8 network, at least in maybe a certain geographic area, to then
9 narrow down to what it thinks is contraband images or videos?

03:53 10 A. Right. In order to discriminate between contraband and
11 noncontraband, it has to get all of the messages. It doesn't
12 see all of the BitTorrent traffic in the entire world, but it
13 certainly sees whatever is in its neighborhood and what it --
14 you know, whatever its peers are interacting with. And it then
03:53 15 sifts through that to look for ones that are, you know,
16 potentially bad.

17 Q. And this could maybe be important, for example, for raising
18 Fourth Amendment concerns?

19 A. Well, one interesting question is, okay, there's this
03:54 20 database of -- of known hash values. How do things get --
21 what's the process for adding things to that database? How
22 rigorously are they vetted? Is the database --

23 I mean, it's also easily possible to imagine this
24 database being used for discovering things other than child
03:57 25 pornography. You could use it to look for hashes that are

1 associated with, say, recipes for bombs or things like that.
2 It's not just a -- it's a Swiss army knife tool in the right
3 hands.

4 And so, I mean, I'm not a criminal law practitioner so
03:57 5 I'll leave the Fourth Amendment arguing to you, but, yes, it
6 seems to me that this is -- the fact that it looks at both
7 legitimate and non-legitimate traffic in order to figure out
8 what the non-legitimate traffic is, you know, that is -- that
9 seems invasive to me. But, again, I'm -- that's not the part
03:58 10 I'm an expert on.

11 Q. Now, you also want to -- and we've talked about this a
12 little bit already with the false positives, but you want to be
13 able to have access to the program to test its accuracy and
14 reliability in how it carries out its methods, correct?

03:58 15 A. Correct.

16 Q. All right. And this would be important because every
17 software program has certain parameters and instructions that
18 should be followed to make sure it's being used correctly.

19 A. Right. So the analogy I would make here is to say a radar
03:58 20 gun or a breathalyzer. These are tools that are used to
21 establish probable cause to charge people with crimes or at
22 least ordinance violations. And, but we know that they have to
23 be calibrated a certain way and they have to be used correctly.
24 And so defense attorneys routinely verify that that has been
03:59 25 done. You know, it is a defense in many cases if the equipment

1 was not operated correctly.

2 And we have no way of knowing what questions to even
3 ask here, because we don't know how the software is set up, how
4 the software is installed, what the correct way of operating the
04:00 5 software is. Those are all things that are opaque to us. And
6 so we don't have any way of evaluating or even properly
7 questioning a prosecution witness about whether that took place
8 in this case or not.

9 Q. Could you just describe briefly for the Court, if you were
04:00 10 able to get access to the program, like what are some of the
11 things that you might try to do or try to -- you know, what kind
12 of tests might you run?

13 A. Well, one of them would be just what's called packet
14 capturing or packet sniffing. I would attempt to watch from a
04:00 15 nearby place on the network a single source download and see if
16 indeed it all came from a single source. Probably do that a few
17 times just to verify that it doesn't every so often grab a piece
18 from elsewhere.

19 I would also watch when the software generates an
04:01 20 alert what traffic caused it to do that. That would -- those
21 would be things that would help me understand what it's doing
22 under the hood. And that's kind of the goal here.

23 Q. Now, would it matter where you did this testing or review,
24 whether it was at, you know, your own facility, your office
04:01 25 versus perhaps in a law enforcement office?

1 A. I have no, you know -- it would be more convenient at my
2 office, but I have no, you know, principled objection to doing
3 it elsewhere.

04:01 4 I would say that if it were at another facility, I'd
5 probably want to schedule more than one visit because I assume I
6 would spend a fair amount of time getting up to speed on just
7 what -- how I would do the tests there. You know, what's
8 available to me in terms of network ports or, you know, power
9 outlets, you know, sort of mundane things like that. Also, just
04:02 10 learning how to -- I've never seen the software. I don't know
11 what it looks like. I don't know the first thing about how to
12 launch it or do anything like that. So I'd need a little time
13 to just get oriented, and then I'd also need time to do the
14 tests.

04:02 15 So doing it at my leisure at my own facility would
16 make that easier, but it's not impossible to do it elsewhere.
17 I'd just need the requisite degree of access.

18 Q. Now, would you view it as a problem if this was done
19 pursuant to a protective order where you can't disseminate or
04:02 20 discuss or otherwise disclose the program to anybody else except
21 for me?

22 A. No, I believe we've even proposed that.

23 Q. So you would obviously -- I mean, you're a practicing lawyer
24 in Wisconsin, correct?

04:03 25 A. I am.

1 Q. You value your law license. You wouldn't do anything to
2 violate an order, right?

3 A. I'd do my best to avoid that.

4 Q. Okay. Another reason that you might want access to the
04:03 5 program would be, again, to ensure that it -- when it identifies
6 a computer as flagged for possessing a torrent, okay? That that
7 is maybe different than an actual child pornography image or
8 video, right?

9 A. Right. Now, this would be probably a dicey thing to test,
04:03 10 since I don't possess any child pornography and have no
11 intention of doing so, so we'd probably have to set up some way
12 of having a known, you know, safe file, you know, some dummy
13 file that we could pretend was something, you know, that
14 Torrential Downpour would alert on. So we'd want to see when
04:04 15 that file gets shared what is it that triggers Torrential
16 Downpour to alert and do the log entries that it creates
17 accurately reflect the condition that was present on the
18 network.

19 Q. You mentioned earlier, but I just want to maybe clarify this
04:04 20 a little bit more. So it's virtually impossible for us as the
21 defense to prepare any sort of cross-examination of government
22 witnesses about how this program is used or whether it was used
23 correctly or within the right parameters, right?

24 A. The best we have right now is what's in warrant applications
04:04 25 and then a few inferences we can draw from there.

1 There's a little bit of literature, you know,
2 presentations that one can download, but there's really not
3 much -- we don't have access to documentation about the system.
4 We certainly don't have the source code. No one outside of law
04:05 5 enforcement to my knowledge has seen a working copy of the
6 software.

7 We get conceptually what it is, and we understand that
8 a system could be built to do what it claims it does, we just
9 have no way of verifying it. And that makes it hard to know
04:05 10 what questions to ask, again, about whether the system was
11 properly installed, was it properly operated, what network
12 environment does it require in order to function correctly, did
13 it have that at the time. These are all questions we don't --
14 since we don't know information about the guts of the system, we
04:05 15 don't know what questions to ask. And we could ask a question,
16 but we wouldn't know whether the answer was helpful or not.

17 Q. So would it be fair to say that your opinion is we are
18 basically at the mercy of the government right now of what they
19 say it does and doesn't do without independently verifying it?

04:05 20 A. Very much so. The -- we have nothing -- we just are -- we
21 either take on faith what's in the warrant application or we
22 don't.

23 Q. And so there's really been no -- again, as far as you're
24 aware, and this is anywhere in the country -- any adversarial
04:06 25 testing of this program.

1 A. I am not aware of any. There are a couple of competitors to
2 Torrential Downpour also which are closely guarded. I'm aware
3 of efforts in various courtrooms to get varying degrees of
4 access to Torrential Downpour and other systems. I'm unaware of
04:07 5 someone getting unrestricted access to do just sort of thorough
6 testing.

7 Q. And lastly, would it be important to gain access to the
8 program so that we can perhaps try to figure out why the file
9 that the program said it downloaded twice over the course of two
04:07 10 different days is not located on Mr. Owens' computer?

11 A. Well, what we could do -- I mean, we know that the program
12 said it downloaded those things, and we know that the file was
13 not present at the time when the computer was seized. We can
14 think of a variety of explanations for why that might be the
04:08 15 case. Inspecting the software would help us evaluate sort of
16 which inferences are more plausible versus less plausible.

17 MR. DONOVAN: Your Honor, I believe I'm done. If I
18 could just check my notes for a quick minute here to see if I
19 missed anything.

04:08 20 (Brief pause.)

21 MR. DONOVAN: Your Honor, I have no further questions.

22 THE COURT: Okay. Mr. Humble?

23 CROSS-EXAMINATION

24 BY MR. HUMBLE:

04:12 25 Q. Mr. Engel, you mentioned your background and training. Have

1 you had any or received any training in BitTorrent file sharing
2 for the networks?

3 A. Other than experiential testing, no.

4 Q. Okay. And you also mentioned that it sounds like what you
04:13 5 learned you learned from reading the literature and also doing?

6 A. Yes. For better or worse, people of my vintage typically
7 the courses weren't available at the time when we needed to
8 learn things, so we had to just go do it.

9 Q. Okay. And you mentioned that some of the literature upon
04:13 10 which you relied to teach yourself was authored by this
11 gentleman sitting next to me; is that correct?

12 A. Yes. You have next to you one of the probably half dozen
13 people in the world who knows most about the software.

14 Q. Okay. So if he helped teach you about what you know about
04:14 15 BitTorrent, do you have reason to trust his -- distrust his
16 expertise in this area with regard to BitTorrent Torrential
17 Downpour or Torrential Downpour Receptor?

18 A. Curious question. I don't distrust him. No, I have no
19 reason to distrust him. I mean, I don't think he's trying to
04:14 20 fool anybody. I just don't have any objective way of verifying
21 any of the facts in this case.

22 Q. But, again, what you've learned about this essentially, at
23 least in part, you've learned from this gentleman. So you would
24 rely on his expertise in what you're testifying to here today
04:14 25 essentially.

1 A. In part, yes.

2 Q. And you referred to this in your -- in your affidavit as
3 "RoundUp" and you clarified "Torrential Downpour." It's
4 actually Torrential Downpour Receptor, were you aware of that?

04:15 5 A. I'm aware of that term as well.

6 Q. Can you tell the Court the difference between Torrential
7 Downpour and Torrential Downpour Receptor?

8 A. Not with specificity I cannot.

9 Q. Okay. And when you had the opportunity to review the logs
04:15 10 and the imaging of the computer, you said that you never found
11 this image that is alleged in the indictment; is that correct?

12 A. That image as far as I could tell was not present on the
13 computer.

14 Q. And I said "image" and earlier you said "image," but
04:15 15 actually, more correctly, it's a movie.

16 A. Yes. Yes.

17 Q. Okay. So you didn't find this movie, but you did review the
18 logs, correct?

19 A. Yes.

04:15 20 Q. And those logs did reflect that I believe there were 226
21 portions that made up the movie for lack -- I say "portions" for
22 lack of a better term?

23 A. I'm taking your word for the number 226. But, yes, the
24 movie was reflected in the logs.

04:17 25 Q. And this will probably be an exhibit soon, but this log

1 essentially shows all 226 portions of that movie are going into
2 the computer of Mr. Owens; is that correct?

3 A. That log is a document that speaks for itself. I don't have
4 a way of assessing its accuracy, but it has entries that appear
04:17 5 to be what you describe.

6 Q. Do you have a way of proving inaccuracies in the log?

7 A. No.

8 Q. Okay. With regard to your review of the logs and the mirror
9 imaging of Mr. Owens's computer, did you find evidence that that
04:17 10 movie had been on Mr. Owens's computer?

11 A. I saw an indication that it may have been there, yes.

12 Q. And did you find indications that that particular movie with
13 that particular hash value may have actually been on Mr. Owens's
14 computer at different times throughout 2018, 2016, 2017?

04:18 15 A. I don't believe -- or at least I don't recall, sitting here
16 today, seeing anything that gave me a sense of the time at which
17 it may or may not have been there. I did find a reference to
18 the file name, but that's all I recall finding.

19 Q. Okay. And in looking at, again, the evidence, the computer,
04:18 20 the forensic evidence, were you able to establish essentially
21 any evidence -- or did you observe any evidence that the file
22 had been there prior to Mr. Owens's computer connecting with law
23 enforcement?

24 A. Again, I don't recall what I saw being associated with a
04:19 25 time. So I'm not -- one can always imagine a forensic analyst

1 smarter than oneself, so I'm not saying that there was
2 definitively no such evidence. I just -- what I recall was
3 seeing a reference to the file name and I did not recall that
4 having any kind of timestamp on it.

04:19 5 Q. And in reviewing that information did you -- well, I'll just
6 ask you: Do you know what program Mr. Owens used to establish
7 peer-to-peer communication?

8 A. It's in my notes, but I don't recall if it was Micro-Torrent
9 or what.

04:22 10 Q. Okay. And did you see any evidence when you were reviewing
11 the forensic materials that Mr. Owens had downloaded a
12 peer-to-peer program very close in time to when he connected
13 with law enforcement?

14 A. There was peer-to-peer software installed. That would have
04:22 15 had a timestamp on it. I don't recall sitting here right now
16 the proximity. I could refresh my recollection and I would -- I
17 don't -- I don't have any reason to dispute it.

18 Q. Do you recall in reviewing that information that that
19 particular movie with its 226 portions was -- that there was
04:23 20 evidence that it was on Mr. Owens's computer after he
21 established contact with law enforcement?

22 A. Again, the evidence I saw for the existence of that file, I
23 don't recall any time data associated with it. So, no, I don't.
24 All I saw was the file name.

04:23 25 Q. Well, let me ask you this. If -- if there was evidence that

1 this particular movie was on Mr. Owens's computer prior to
2 connecting with law enforcement, and there was -- and I'm just
3 asking you to go with the question -- and there was evidence
4 that this particular movie was on Mr. Owens's computer after
04:23 5 connecting with law enforcement, would that be pretty good
6 evidence that that particular movie had been on Mr. Owens's
7 computer?

8 A. If there was -- if there was evidence that the file was
9 present before connecting with law enforcement and evidence that
04:23 10 the file was connected -- was present after connecting to law
11 enforcement, would I infer that the file was present?

12 Q. Yes.

13 A. Yes. If the file was present it was present.

14 Q. So people can delete files, correct?

04:24 15 A. Correct.

16 Q. And you've been on other child pornography cases. You've
17 testified you've done the research, looked at the forensics,
18 correct?

19 A. Yes.

04:24 20 Q. Have you seen other instances where individuals who have
21 contraband or child pornography have deleted the images after
22 viewing them?

23 A. I have seen instances --

24 Well, let me answer it -- a two-part answer to that.

04:24 25 The short answer is, of course, people delete files from time to

1 time. And sometimes you'll find traces of files in unallocated
2 space and those are presumably deleted files.

3 I am also aware of times when, as here, in the warrant
4 application there's a report of a single source download of a
04:25 5 file and we don't find it present on the target system when we
6 go to analyze it. I don't know why that is. Deletion is one
7 possible explanation, but another one would be a false positive.

8 Q. This is going to come across very crude, because it is
9 crude, but it's a term that you may be familiar with and I'm
04:25 10 going to ask you: Have you -- are you familiar with the term
11 "pump and dump"?

12 A. No, I'm not.

13 Q. Not with regard to child pornography or the downloading of
14 child pornography?

04:25 15 A. That is -- that's not one I've encountered.

16 Q. Okay. In reviewing the forensic evidence here in this
17 particular case, was there a question in your mind that it was
18 Mr. Owens's computer who initiated contact with law enforcement?

19 A. I don't know of a way from the forensic image to determine
04:26 20 that. So it wasn't a question I particularly investigated
21 because I had no idea how to investigate it.

22 So I -- I'm not sure what would cause a computer to
23 connect to a law enforcement computer just in the abstract. So
24 in that sense I wonder about it, but it was not something that I
04:26 25 investigated.

1 Q. Are you familiar with the term "seeding"?

2 A. Yes.

3 Q. Could you describe for the Court what seeding is?

04:27 4 A. In broad terms it's advertising the presence of files so
5 that you can -- you're participating in the network and people
6 know that you've got either whole files or at least segments of
7 files that others might want.

8 Q. And seeding essentially -- well, sometimes, if not most
9 times, seeding is done by someone who already possesses an image
04:27 10 or a movie; isn't that correct?

11 A. My understanding -- yes. Yes, that's correct.

12 THE COURT: This is s-e-e-d-i-n-g?

13 MR. HUMBLE: Yes. Seeding as in -- S, yeah.

14 THE COURT: As in lawn seed.

04:27 15 MR. HUMBLE: Yes, correct.

16 BY MR. HUMBLE:

17 Q. So that seems counterintuitive. If someone already has the
18 movie, why are they offering it out to the world?

19 A. That's sort of the economic principle that's central to
04:27 20 BitTorrent. What one downloads one ought to offer for sharing.
21 And that's sort of how the BitTorrent network maintains itself
22 as an efficient distributor of files.

23 Q. So essentially that almost certainly is why the term is
24 called seeding. So you just keep distributing and distributing
04:28 25 and distributing because you're hoping it's going to come back

1 to you.

2 A. Not the same file, but --

3 Q. Not the same file, correct.

4 A. Yes.

04:28 5 Q. Same genre.

6 A. Well, genre even -- I think it's just bandwidth. I don't
7 know that it discriminates by subject matter so much as just if
8 you're not offering things, then you're kind of a jerk user of
9 the system and you shouldn't get the benefit of it.

04:28 10 Q. Okay. And what is swarming?

11 A. Swarming is another feature of -- I think it was first in
12 Gnutella. It's a way of boosting the performance of downloads
13 of certain files. I'm afraid, sitting here right now, I can't
14 go into much more detail than that. I don't recall exactly how
04:29 15 swarming works on BitTorrent.

16 MR. HUMBLE: I don't have any further questions,
17 Your Honor.

18 THE COURT: Mr. Donovan?

19 MR. DONOVAN: Just a couple follow-up, Your Honor.

04:29 20 REDIRECT EXAMINATION

21 BY MR. DONOVAN:

22 Q. So, Mr. Humble asked you about how part of your knowledge
23 and expertise of BitTorrent is based on the government's
24 witness, correct?

04:29 25 A. Or documents authored by him. I've never met him before

1 today.

2 Q. Correct, I'm sorry. To be more precise, documents authored
3 by him.

4 A. Yes.

04:29 5 Q. And again, I just wanted to clarify, there is no independent
6 access to this program.

7 A. That's correct.

8 Q. And so anything that's known about this program is either
9 what is chosen to be shared by its authors, including the
04:30 10 government witness, or that comes out through litigation.

11 A. Yes.

12 Q. Like, for example, in case decisions or, you know, opinions
13 and orders, things like that.

14 A. Yes. And one can glean tidbits here and there from things
04:30 15 like warrant applications.

16 Q. So I guess my question -- you might be -- you know, where
17 else could you go to learn about this? Other than perhaps
18 publications by the government witness.

19 A. If I knew of another place I'd go there.

04:30 20 Q. Okay. The government asked you questions about whether you
21 have any reason to doubt that the logs are inaccurate. Okay?

22 Again, why can't you assess the logs separate from the
23 program?

24 A. Well, the log is just a text file. Sitting at my computer
04:31 25 with a Notepad application, I can make a text file that says

1 darned near anything. I don't think the government is
2 generating false text files. That's not -- I'm not that much of
3 a conspiracy theorist. But it seems to me antithetical to the
4 idea of criminal defense that we should just take it at face
04:31 5 value. It seems that we should be able to do some investigation
6 of the degree to which it accurately reflects the events that
7 it's reported.

8 Q. Would it be fair to say that if there's problems within the
9 program itself then there might be problems within the logs
04:31 10 themselves?

11 A. Right. That's the old "computer garbage in/garbage out"
12 theory. If the software does not function as designed, then
13 there's no reason to expect that the logs would be better than
14 the program itself.

04:32 15 Q. You testified that again you reviewed the forensic evidence
16 available in this case personally.

17 A. Yes.

18 Q. And you found indications of perhaps the file name of the
19 movie that was supposedly downloaded on Mr. Owens' computer.

04:32 20 A. Correct.

21 Q. But no actual file.

22 A. Correct.

23 Q. And I apologize, I forget, did you find any indications of a
24 hash for that movie?

04:32 25 A. I did not.

1 Q. Okay. Now, part of these peer-to-peer programs would be,
2 again, a search function where like a term could be entered,
3 correct?

4 A. Yes.

04:32 5 Q. And so would that be part of a Torrent? So like could a
6 search term or a function be part of a Torrent that might be on
7 the computer? Meaning that, you know, it might say it's looking
8 for or has information on it but, again, doesn't have the file
9 itself?

04:33 10 A. Yes. One can find, for example, Torrent files on a
11 computer, but not the -- not the movies or images or whatever
12 that the torrent files would enable you to acquire.

13 Q. Okay. And so, again, you said one explanation could be, as
14 you acknowledged, that the user deleted the file, right?

04:33 15 A. Yes.

16 Q. But another explanation could be, again, this idea of a
17 false positive that perhaps Torrential Downpour reporting a
18 single source download was just wrong; that there -- you know,
19 it reports a download, but there never was a file there to
04:34 20 download from.

21 A. Correct.

22 Q. Okay.

23 MR. DONOVAN: I don't have any other questions,
24 Your Honor.

04:34 25 THE COURT: Okay. Thank you, Mr. Engel. You can step

1 down.

2 (Witness excused at 2:44 p.m.)

3 THE COURT: How about a short break. Do you have -- I
4 mean, are we in a rush because a witness has to catch something
04:34 5 or get out of here or --

6 MR. ERDELY: 6:45.

7 MR. HUMBLE: We've got some time, Your Honor.

8 THE COURT: 6:45?

9 MR. HUMBLE: It's Green Bay, we can get him over
04:34 10 there.

11 THE COURT: 20 minutes.

12 (Recess taken at 2:45 p.m., until 2:58 p.m.)

13 THE CLERK: Please raise your right hand.

14 Do you solemnly swear the testimony you are about to
07:17 15 give is the truth, the whole truth and nothing but the truth so
16 help you God?

17 THE WITNESS: I do.

18 THE COURT: Please state and spell your first and last
19 name for the record.

07:17 20 THE WITNESS: Robert Erdely, E-r-d-e-l-y.

21 THE COURT: Thank you, Mr. Erdely.

22 Go ahead, Mr. Humble, you may proceed.

23 MR. HUMBLE: Thank you. May I approach the witness,
24 Your Honor?

07:18 25 THE COURT: You may.

ROBERT ERDELY, GOVERNMENT WITNESS, DULY SWORN

DIRECT EXAMINATION

BY MR. HUMBLE:

Q. Mr. Erdely, I'm just going to hand you what's been marked as Exhibit 1, can you just tell me what that is?

A. It's a copy of my CV.

(TRANSCRIBER NOTE: Mr. Humble not near a microphone.)

Q. [Indiscernible]?

A. I did.

MR. HUMBLE: [Indiscernible].

MR. DONOVAN: No objection.

THE COURT: 1 is received.

(Exhibit 1 received in evidence.)

BY MR. HUMBLE:

Q. If you could go ahead and just inform the Court, what is your background, who is your employer, how long have you been employed, that kind of thing?

A. I worked for the Pennsylvania State Police until I retired in 2012. The last five years of that career I supervised the Computer Crime Unit. And it was during my time with Computer Crime Unit that I worked on the development of these tools with the University.

And, April 2012 I retired and the very next day I started with the Indiana County Detectives Bureau where I kept the same role — computer crime investigations, which is both the

1 investigative piece and the forensic analysis piece.

2 So as part of that and my time with Computer Crime
3 Unit, I went through various trainings, conferences and such
4 where I was able to acquire professional certifications. For
07:21 5 instance, the CISSP certification the defense expert was
6 speaking of, I obtained that.

7 I'm a Microsoft certified systems engineer, a Cisco
8 certified networking professional.

9 I went through the certification process for four --
07:25 10 four different certification processes for computer forensics.
11 And, again, just the ongoing training day to day.

12 As it relates to peer-to-peer, much of my training
13 came from the University, the researchers, the professors and
14 Ph.D.'s that did the research into the network so I could learn
07:26 15 exactly how it operates.

16 Q. Okay. Just total, how many years have you been dealing in
17 investigating computer crimes?

18 A. I started with the Computer Crime Unit October 1998 to
19 present.

07:26 20 Q. Okay. And is it fair to say that now you split your time
21 between investigations and training and testifying?

22 A. Correct. I do trainings for the Internet Crimes Against
23 Children Task Force, for the FBI's Violent Crimes Task Force,
24 their international task force. I've done a training for
07:27 25 Interpol and various different countries. I provided this

1 technology beyond the United States.

2 Q. So as you say, you've trained on BitTorrent and the
3 investigative use of BitTorrent in other countries. How many
4 countries use this investigative Torrential Downpour?

07:28 5 A. We last checked, over 60 countries used our investigative
6 systems.

7 Q. And if you could just kind of describe for the judge when --
8 in defense affidavit and probably in your resume, it references
9 Amherst is where this particular software was developed. Sounds
07:28 10 like you were in on the ground floor. Can you explain that to
11 the Court?

12 A. Yes. Initially there was research done by a professor from
13 University of Massachusetts Amherst, and a professor from
14 Georgetown University. That was the initial discussions as to
07:29 15 where we move next as law enforcement for investigations.

16 After that, I worked, you know, day in and day out
17 with the senior programmer at University of Massachusetts
18 Amherst where we did the development of the software.

19 Q. So you didn't author the software.

07:29 20 A. No. I was part -- the development team was myself and the
21 senior programmer from UMass.

22 There's a lot of back-end work that relate to other
23 aspects and other networks that we investigate that I programmed
24 in that area. I'm a Microsoft data -- Certified Database
07:29 25 Administrator, so I work with the databases and things like

1 that, as well as the actual individual testing of the software
2 before it's deployed.

3 Q. Okay. So fair to say you're very familiar with Torrential
4 Downpour.

07:30 5 A. Yes.

6 Q. Okay. And Torrential Downpour Receptor?

7 A. Yes, sir. Those are two separate programs. And this case
8 relates to one, which is Torrential Downpour Receptor,
9 specifically version 1.50.

07:30 10 Q. Okay. We've heard about the basics of BitTorrent from the
11 defense expert. Is there anything that you want to clarify or
12 put a little more focus on for the Court with regard to how that
13 operates?

14 A. Just quickly a high-level -- I just want to make sure the
07:31 15 Court has a good understanding as to how things worked.

16 BitTorrent is different as was already described. One
17 of the major differences is that the torrent file that we've
18 heard about is a set of instructions on how to get the actual
19 files that they describe.

07:31 20 Well, you have to search outside websites or get them
21 from other people. The BitTorrent software, although it gives
22 you a mechanism to type and search as described, I just wanted
23 to clarify the BitTorrent file sharing network doesn't have a
24 searching component built in. When I type in the little search
07:32 25 field in this program, which is my BitTorrent software,

1 typically what happens is a web browser just pops up and starts
2 giving you your search results. Well, you could have skipped
3 that whole step and just went to your web browser, opened up
4 Google, and started searching that way.

07:32 5 So I just wanted to be clear that there is no
6 mechanism to search by file name within the BitTorrent file
7 sharing network. So that was a little bit different.

8 The second -- so after I get the instructions I search
9 the internet and I find a torrent file that describes the
07:33 10 content I'm looking for. Then you load that torrent --

11 Q. Can I just stop you there?

12 A. Yes.

13 Q. We're talking in the abstract. What might one put into this
14 to find the type of movie or image they are looking for?

07:33 15 A. "Jurassic Park movie torrent."

16 Q. Okay.

17 A. If I just use those four key words I would be presented with
18 lots of sites that have these instruction files, these torrent
19 files that would enable me to download Jurassic World or any of
07:34 20 the other new movies that are out there. But you have to start
21 by finding these instructions outside of the BitTorrent file
22 sharing network is my point.

23 Q. Okay. So now I found these websites, and I'm assuming the
24 same holds for erotica or child pornography or any type of other
07:34 25 file?

1 A. Yes, sir.

2 Q. I found this, I found what I want, how do I go about getting
3 it with the BitTorrent?

4 A. So now what happens is you load that torrent file into your
07:34 5 BitTorrent program. Much like if you wanted to open up a Word
6 document. You can either double-click it and it will launch the
7 program and load the Word file you were trying to view. Well,
8 with BitTorrent it's similar, I can double-click the torrent
9 file and, assuming there's an association between those two, it
07:35 10 just opens up my BitTorrent program and starts working.

11 Or you could have it already open and choose the
12 drop-down file, open, and you just navigate to that torrent file
13 which are the instructions. But in either case, once the
14 torrent file, the instruction gets loaded into the program,
07:35 15 searching does happen. And what searching happens is, that now
16 my computer, running a BitTorrent piece of software that has
17 instructions loaded, it goes out to the BitTorrent network.

18 There's indexing that happens. So the BitTorrent
19 network keeps track of who is associated with which torrent.
07:36 20 Because if I load a torrent, I need to find other people that
21 have some or all of that material to share with me. I just
22 started, I have nothing to share.

23 So the BitTorrent network does that all by itself.
24 And it's just a search for a torrent that I've now loaded into
07:36 25 my program which is different than initially finding that

1 torrent. They are two separate things.

2 Q. So when you say it does it all by itself -- I guess that was
3 a corny commercial where they said "set it and forget it"? I
4 mean, is that what we're talking about? You've already told it
07:36 5 what you want and you can just walk away and it's going to ask
6 all of the people all over the world through the internet to
7 give you pieces of what you want?

8 A. Correct. I load it into my program, assuming that all the
9 [Indiscernible] are in place, it's going to learn a list of IP
07:37 10 addresses that potentially -- that have shown this association,
11 they've communicated on the BitTorrent network asking about the
12 same torrent file. So they basically are matchmakers at this
13 point. The BitTorrent network says this is the torrent you're
14 looking for, I understand that, here's a list of 40 or 50 IP
07:37 15 addresses that also show that association.

16 Well, at the point -- and this is very important -- at
17 the point in time where my computer has interacted with the
18 BitTorrent file sharing network and expressed interest in this
19 torrent file, which is identified through caching like the Court
07:38 20 has already heard, a very unique way to identify content.

21 So it will keep track of the fact that I asked that
22 question. So my computer had -- my BitTorrent software, I
23 loaded a torrent file into it, I've made an inquiry to the
24 network, now the network knows about me. I have an association.
07:38 25 And it could be me, Rob Erdely the law enforcement officer, or

1 any other BitTorrent user in the world.

2 So the next thing that happens is, I will start trying
3 to connect people to get pieces of the file or files -- because
4 it could be one file or many files described by a torrent -- and
07:39 5 hopefully get to connect to people. And at the point in time we
6 connect, what happens with this BitTorrent file sharing network,
7 there's some handshaking that goes on. It's just a computer
8 term, but basically we're just gonna have a little conversation
9 before we start creating data. And one of the very first things
07:39 10 that happens is, regardless of whether I initiated the
11 connection to you or you initiated the connection to me, we
12 first have to agree upon one thing: That we're talking about
13 the same torrent.

14 And the torrent's identified through something called
07:39 15 an "info hash," but very simply it's a very, very, very unique
16 way to identify it. It's more unique than DNA is to the human
17 body. That's how unique it is.

18 So we agree we're talking about the same torrent. And
19 then the next thing that happens is, both computers, regardless
07:40 20 of -- if I contacted you because I needed pieces of data, or if
21 you contacted me because you needed pieces of data, in either
22 case both sides are required to report, "These are the pieces I
23 have to share," and the other side says, "These are the pieces I
24 have to share."

07:40 25 Because BitTorrent is built on the premise it's a

1 tit-for-tat exchange. You're supposed to be able to give pieces
2 of data to a person that is connected to you to download data,
3 as well as receive. You're supposed to give and get, all
4 through the same connection. And it's an automatic thing that
07:41 5 happens.

6 Q. Let me ask -- let me stop you there. Sorry.

7 Do I always need to go to 50 or 100 different people
8 to get little pieces? Can I not just get the Jurassic Park
9 movie I want from one person?

07:41 10 A. You could and do at times on the BitTorrent network using
11 any software, not law enforcement, nothing specific. The
12 network allows for the entire content to be downloaded from a
13 single IP address.

14 But, it is true that you will speed up your download
07:42 15 times if you reach out to two, three, four, 10 or 20 different
16 computers, because all of them could be giving you data at the
17 same time.

18 But, just to put it in perspective, if I'm -- if I
19 load a torrent into my BitTorrent program and I'm seeking to
07:42 20 download that material and there's only one person online that
21 has it available at that moment in time, then the entire
22 download happens from a single sharing computer. It's nothing
23 unique to law enforcement software that downloads happen from a
24 single sharing client.

07:43 25 Additionally, if you think about the person that had

1 to create this collection of data to share, no one else in the
2 world has it. I'm creating this unique collection of files. So
3 there's a process within your BitTorrent software to create that
4 instruction file, that torrent file. So when I start sharing
07:43 5 that torrent file out and people want to start downloading it,
6 there's only one person in the world that has that collection of
7 files, me, the creator, until I start sharing it out.

8 So my point is, the fact that law enforcement does a
9 download from a single sharing IP address is not unique to law
07:44 10 enforcement. It happens naturally on the BitTorrent file share
11 network on a daily basis. So....

12 Q. So is that the conclusion of your overview of BitTorrent?

13 A. No. So then I just learned to go a step further. There was
14 already a definition given for seeding and I just want to make
07:50 15 sure the Court understands exactly what seeding is.

16 So if I loaded a torrent into my BitTorrent software
17 and I downloaded everything, now I have all the files that are
18 described by that torrent file. I need nothing more. That's
19 the moment in time you become a seed. If you are seeding a
07:50 20 torrent, you're in a position where you've -- you possess it
21 all. And you're staying online for the purpose of continuing to
22 seed the data, like a farmer in a field throwing seeds to grow
23 his crops. Because a torrent and its associated data will only
24 be available assuming there's enough BitTorrent programs online
07:50 25 around the world that have those pieces to share.

1 Well, so now that I have it all, this is the point
2 that I'm trying to bring out, I am making myself --

3 (TRANSCRIBER NOTE: Witness moves away from microphone
4 or microphone not functioning.)

07:51 5 -- available to anybody looking for that torrent and I
6 will share the data for them. But it's important to understand
7 this. I'm not just sitting here passively waiting for people to
8 find their way through the internet to connect to my computer.

9 That certainly is one of the two possibilities.
07:51 10 Someone loads a torrent, they want to find a down -- someone to
11 download it from, the BitTorrent network, the index tells them
12 about my IP address, so they connect to me. And I'll give them
13 the pieces they request.

14 Again, I don't need anything, I have everything, so
07:52 15 that whole tit for tat stage is gone, it's out the window. But
16 there's another thing that happens, and a lot of people don't
17 realize it [Indiscernible].

18 I don't just sit there as a seed on the BitTorrent
19 network when I have everything and just sit passively waiting.
07:53 20 No. I created the index and look for people that are still in
21 need of some of this material I have. I'm being overly helpful.
22 I will make outbound connections from my computer -- when I say
23 "I," I'm talking about the BitTorrent [Indiscernible] I
24 apologize. I'm not trying to infer that the person
07:53 25 [Indiscernible] to make it happen. But the BitTorrent network,

1 I'm a seed, will continually query the network looking for new
2 IP addresses that are in need of data. And I'm going to deliver
3 it to them. I'm going to knock on the door and say, "I heard
4 you need some of this data" and offer it up to them.

07:54 5 So it makes outbound connections to computers all
6 around the world and it continues to share, and it didn't
7 require that computer to reach into my BitTorrent software and
8 make the request. I'm delivering it to you. It's home delivery
9 so to speak.

07:55 10 Q. Okay. So when all this is happening, this happens
11 automatically if the computer is on and connected to the
12 internet?

13 A. Correct. As long as it's connected to the internet and it's
14 running the BitTorrent software and until the person chooses to
07:55 15 stop the sharing or seeding process, it would continue operating
16 that batch.

17 Q. And the handshake, the handshake takes place mutually, for
18 lack of a better image, outside of each computer? I mean, no
19 one's intruding each other's computer to go ahead and do that,
07:56 20 is it?

21 A. No, it's expected. The two computers have something called
22 a TCP connection. It just -- think of it like a tunnel. There
23 isn't a connection established or even a phone call. I pick up
24 the phone and I dial your number and you have a phone, we have
07:56 25 an established connection, I can talk to you and you can talk to

1 me. That's what happens on BitTorrent.

2 So either I connect to the computer or the computer
3 connects to me, but at that point we have this open line of
4 communication. And again, the first thing that's gonna happen
07:57 5 is, we're going to agree that we both are talking about the same
6 torrent. Because if we're not, the conversation's over. He
7 could have stopped sharing. He could have stop [Indiscernible]
8 seeding [Indiscernible].

9 The next thing that happens is handshake. And that's
07:58 10 where one BitTorrent program can talk to the other BitTorrent
11 program and tell each other: I'm running a BitTorrent program
12 called BitComet, and I could respond I'm running a BitTorrent
13 program called UTorrent. Those are both real clients. So
14 that's part of the handshake.

07:58 15 It's available to any program. As a matter of fact,
16 the off-the-shelf, so to speak, clients tell you that. Or if
17 there's a tab that says peers and you can see their IP address,
18 you can see the version of software that they told us that they
19 were running. It's part of the normal everyday communication,
07:59 20 that handshaking. It tells us what networking port they listed
21 on, all those sorts of information.

22 Q. Okay. So Torrential Downpour Receptor, which is the program
23 we're talking about here with regard to Mr. Owens, how does that
24 differ from the BitTorrent -- or does it differ from the
08:00 25 BitTorrent that you just described?

1 A. Well, it's using just the functions I just described.
2 Obviously we're law enforcement, that's not a surprise. But the
3 way BitTorrent -- I'm sorry, Torrential Downpour Receptor works
4 is that it searches for torrents files, the instructions, that
08:00 5 are known to law enforcement. And who is the person that
6 decides whether it is something we search for or not? It's me.

7 And we learn that through the hashing of the files and
8 comparing it to other [Indiscernible] location of files we know
9 about, or at times I actually have to physically download the
08:01 10 file and look at them and say that's an eight-year-old, it's a
11 sex offense, we're going to include this on the torrents that we
12 investigate.

13 We do not listen in -- listen or monitor or try to
14 discern one type of traffic from another. We simply search for
08:01 15 a torrent to learn the IP addresses of other -- others who have
16 shown an association with that torrent, and we receive the
17 search results relating to what IPs are present. We do not -- I
18 don't even know how you would do that -- sit there and somehow
19 sniff out or monitor all BitTorrent traffic. It's a
08:02 20 decentral -- decentralized network. That would be an incredibly
21 difficult thing to do if it's possible at all.

22 We are just doing the same messages out that any
23 BitTorrent program would give and receiving responses back.
24 [Indiscernible] receptors you need, because all we're doing is
08:03 25 searching for torrents that relate to child exploitation and

1 then we sit there. We just sit. We're gonna sit and wait.

2 And because I searched for that torrent, remember, the
3 BitTorrent file sharing network knows my IP address
4 [Indiscernible], my law enforcement IP. And the BitTorrent
08:03 5 network is going to tell others about me. I'm just gonna sit
6 and wait.

7 And that's what happened in this case. The suspect
8 computer or the user's computer, however you want to define
9 that, loaded a torrent into their BitTorrent program. The first
08:04 10 step happens where they inquire on the network [Indiscernible],
11 what IPs might I connect to that also have an association with
12 this torrent? And the suspect computer learns my law
13 enforcement IP address and he, or she, connects to us.

14 That's analogous to the drug dealer driving his car to
08:04 15 the police station, going to the front desk and, any police
16 officers here want to buy crack? Because that's what happened.
17 The suspect computer arrived to law enforcement's computer, the
18 TCP connection happens, we both agree that we're willing to talk
19 about the same exact precise torrent, and now both sides, the
08:05 20 person that contacted the investigator and the investigator
21 contacted the person who established the connection, we get to
22 talk freely about that torrent. What pieces do you have to
23 share, the law enforcement computer can ask the suspect
24 computer, and vice versa.

08:06 25 So we're law enforcement, we do not share. And we

1 don't even have to lie. They ask us what pieces we have to
2 share, we say zero. We have none. That's a completely
3 acceptable message on the BitTorrent file sharing network. And
4 then the sharing computer will tell us what pieces they have to
08:06 5 share.

6 So here's what happened in this case as
7 [Indiscernible] reading the law. The suspect computer was
8 seeding. They had all the pieces. They didn't need anything
9 from law enforcement. They connected to us through the overly
08:07 10 helpful image sharing, like I previously described, and once we
11 were connected we just started asking for the pieces of the data
12 that the sharing client was making available. And all that gets
13 memorialized in a log file by Torrential Downpour Receptor.

14 Q. Okay. And you've reviewed those log files prior to your
08:07 15 testimony here today?

16 A. Yes, I have.

17 Q. And we've brought a couple with us?

18 A. Yes. The two in question that were two downloads of the
19 same file spanning two different days.

08:08 20 Q. Okay.

21 MR. HUMBLE: May I approach, Your Honor?

22 THE COURT: You may.

23 MR. HUMBLE: And counsel has these.

24 BY MR. HUMBLE:

08:08 25 Q. Handing you what's been marked Exhibits 2 and 3, they seem

1 to be quite similar, could you explain to the Court what they
2 are and why they're different?

3 A. Well, this is two different investigative sessions. Every
4 investigative session -- every time we accept a connection from
08:08 5 a person -- a person's computer, it gets compartmentalized in
6 its own folder. It lives all by itself.

7 And on two different dates, the same IP address
8 connected to the law enforcement computer, possessing all of the
9 content in complete possession of this movie file, and offered
08:09 10 to share it because that computer was, quote-unquote, seeding.

11 And that's what happened in these cases. And the
12 reason there's two log files is because the first investigation
13 began on May 21st, 2018. The download happened quite quickly,
14 as the Court's already heard. And then the next day on May
08:09 15 22nd, the early-morning hours of May 22nd, that computer still
16 had that material to share and was still offering to share it to
17 the world. Just fortunate for law enforcement that that
18 computer chose to connect to law enforcement's instance of the
19 BitTorrent piece of the file.

08:10 20 MR. HUMBLE: May I approach again, Your Honor? I'm
21 sorry.

22 THE COURT: You may.

23 BY MR. HUMBLE:

24 Q. I'm going to hand you exact duplicates of what you have
10:25 25 there so the Court has a copy and [Indiscernible].

1 A. Thank you.

2 Q. And obviously these are detailed logs. So I don't want you
3 necessarily to dwell on each line, but there's highlighted
4 portions.

10:25 5 Could you explain for the Court the significance of
6 the highlighted sections, why you chose to highlight those and
7 what that essentially means with regard to the program and the
8 memorialization of the program?

9 A. Sure. And so just for the sake of being on the same log at
10:25 10 the same time, let's just describe a download dated May 21st,
11 2018.

12 Q. Which will be Exhibit 2.

13 A. Which is Exhibit -- I don't have -- yeah.

14 Q. You don't have that.

10:26 15 A. Okay, Exhibit 2. So if we all look at that one, then I can
16 explain the highlighted portion.

17 So on May 20th of -- the first highlighted portion on
18 page 1, it says, "Remote client at IP address 104.11.97.37 has
19 connected to us."

10:26 20 Again, there's two possibilities why some BitTorrent
21 computer would connect to us. That's either, A, he's seeking to
22 find pieces he's yet missing, but he'd still share what he had,
23 or he's seeding. I have it all, I want to be overly helpful,
24 I'm going to give this data freely to anyone on the BitTorrent
10:27 25 file share.

1 So I know that a computer is connected to me, but I'm
2 not really sure why until we start communicating. So the second
3 highlighted area, "info hash sent by remote client."

4 So the computer that connected to us has to tell us
10:28 5 why are you even talking to me. Well, I'm talking to you about
6 a very specific torrent, and that has a hash value, it's called
7 an info hash, uniquely identifying that torrent. There can be
8 no duplicate. It's the same -- the odds are astronomical, it's
9 one -- it's two to the hundred and sixtieth power, or one in 1.4
10:29 10 quindecillion, which is one with 48 trailing numbers. It's a
11 very, very large number.

12 Q. So that number that begins 0833, that is the hash value?

13 A. That's the info hash.

14 Q. Info hash?

10:29 15 A. It's the hash of the information, the instructions unique to
16 that torrent. And that's going to be the only payload or
17 content it could describe is that file that it was meant to help
18 you download.

19 Q. And that second highlighted portion appears to be occurring
10:30 20 at essentially the same exact time as the initial connection?

21 A. Yes, it happens. We're talking about computers. It happens
22 very, very quickly. Right.

23 Q. Okay. So what's that next highlighted portion mean?

24 A. The next thing that happens is, handshake data. And this is
10:30 25 where the computer that is connected to us is telling us more

1 information.

2 Now, we know the torrent that they connected to us
3 about, but in the extended handshake it's telling us things like
4 they're listening port. So if we ever wanted to connect back to
10:30 5 them, you need to know not only just an IP address but also a
6 networking port. So P equals and then you see a number, that's
7 their networking port.

8 REQQ, that stands for request Qs. It tells us how many
9 pieces are we -- I'm sorry, how many packets are we permitted to
10:31 10 ask for at any given moment in time. If it's included, we're
11 supposed to abide by that value and we do. And you'll see that
12 here in a minute.

13 It tells us the version of software they're running.
14 This is something they offered to us in the extended handshake.
10:32 15 It's given to any BitTorrent client, not just us.

16 And then it actually tells us our IP address, your IP.
17 That means they're detailing in the handshake who they connected
18 to. Just so there's no misunderstanding, I meant to connect to
19 -- whatever IP address was listed. That would have been the law
10:32 20 enforcement officer.

21 And then the next highlighted portion is why I know it
22 was seeding and needed no data from law enforcement or it would
23 even think to ask for any data from law enforcement or any other
24 BitTorrent client, because the next section says remote client
10:33 25 has all 226 pieces. You have to download 226 pieces of data

1 before you would be in possession of the entire movie file.

2 Q. And I'm sorry to interrupt, but you'd have to -- based on
3 what you previously said, you'd have to do that 50 pieces -- 50
4 packets at a time?

10:34 5 A. 50 packets at a time is how you have to request them, yes.

6 Q. Okay.

7 A. So, and just to put it in context, that's about 50 -- just
8 over 50 megabytes. So it's actually a small file as far as
9 movies go on BitTorrent. 50 megabytes is not that large.

10:46 10 There's hundreds of megabytes of data that's shared in a single
11 movie file.

12 Q. So here we've been talking about abstract kind of strings of
13 alphanumeric -- alphanumeric strings, it looks like in the next
14 highlighted portion we're actually start talking about the
10:47 15 movie's name that you would see on the computer?

16 A. Correct. Now, it's inside of the torrent. The instruction
17 files knows how to name it. It takes the name of the creator.
18 Whoever first shared this content on the BitTorrent file sharing
19 network, it takes that name.

10:48 20 Q. Okay.

21 A. And the file name is -- and it's long, I don't know -- it's
22 on everyone's sheet of paper. 022 Asian-VPHC. It appears in
23 the quotes. That's the file name.

24 Q. Okay.

10:49 25 A. And then the downloads begin in the next highlighted

1 section, it says, "Sent 50 requests." Well, that's because of
2 the extended handshake. The sharing client that came to us to
3 share child pornography said you're allowed to ask for 50
4 packets at a time. So that's what we did. We asked for 50
10:56 5 packets.

6 And then we started asking for the packets and they
7 get received, line by line. I've requested a packet, it's
8 received. I requested a packet, it's received. Had to happen
9 226 times before the investigator would have the entire payload.
10:57 10 So....

11 Q. And are -- on the next -- geez, I don't know how many pages,
12 17 pages long -- in the next series of pages, is that what
13 you're detailing, that each piece going up to 226 --

14 A. Correct.

10:57 15 Q. -- this log reflects that it's been successfully received?

16 A. Correct, yeah. And it's just a couple minutes is all that
17 it took. And then you don't see any more highlighting until
18 page 11 of 17.

19 So, to put it in context, a computer on the BitTorrent
11:30 20 file sharing network came to us and we agreed we're willing to
21 talk about the same info hash, the same form.

22 We asked for pieces of data. Now, you notice in the
23 extended handshake it never told us 226, did it? It didn't say
24 anything about 226 pieces or even the file name of this file.

11:31 25 It's because both ends of the communication has this instruction

1 file. It's required. Without a torrent file, you can't
2 download on the BitTorrent network. You can't just, you know,
3 wander around on someone's computer and say I think I want to
4 download that. It just doesn't work that way.

11:32 5 It only works because we have the same instructions
6 file. And also included --

7 So, well, let me back up. So for the -- for the
8 sharing computer to say I have piece zero through piece 225,
9 which is 226 pieces, tells me right away he's got the torrent,
11:32 10 he has to have the torrent, because I have my copy and sure
11 enough, there's 226 pieces. Either that or it was a really good
12 guess.

13 But now I named the file like the instructions says,
14 but I've downloaded those 226 pieces. And where I'm going is,
11:33 15 on page 11 where that highlighting [Indiscernible], that's a
16 hashing that happens on every piece of data shared. And it
17 comes up with that fingerprint, digital fingerprint as the
18 defense expert described. It's actually a SHA-1 hash. Secure
19 hashing algorithm version 1 hash is what BitTorrent uses.

11:33 20 And it calculates the hash value, the signature for
21 all 226 pieces. And so now what happens is, we are going to
22 compare those hash values and make sure it matches what is in
23 the instruction file of the torrent.

24 We had data set, we calculated the fingerprint, we
11:35 25 look inside the torrent and it matches. I got the right piece

1 of data. It has to be the right piece of data.

2 So for it to not -- for the computer that connected to
3 us offering to share this torrent file to have guessed that it's
4 226 pieces and responded to our 226 requests for data, have that
11:36 5 computer give us that data and then match 226 SHA-1 hash values
6 is inconceivable. The computer had to be in possession of that
7 file and the instruction file, the torrent file, for what I
8 described to have just happened. It's an impossibility. The
9 computer had to have had it.

11:36 10 Q. And to be clear, that computer came to you. So Mr. Owens
11 came to you.

12 A. Correct. And when you say "you," you mean the
13 investigator --

14 Q. I mean the investigator, I'm sorry.

11:37 15 A. But, yes, the investigator running our software -- just
16 because we searched for the torrent, like any other BitTorrent
17 program searches for download candidates, that was enough to
18 make us associated with the torrent that suspects were any
19 computer on the BitTorrent network comes to law enforcement's
11:37 20 version just the same way they would go to any other BitTorrent
21 program [Indiscernible]: Bitcom, uTorrent, Sherazel (phonetic),
22 there's a ton of them out there.

23 Q. And that was Exhibit 2. Exhibit 3 we don't really probably
24 need you to walk through, but why are there two exhibits? This
11:38 25 one reflects a date of May 22nd.

1 A. Yes. It was -- the Torrential Downpour Receptor is
2 configured by the end-user and you can specify what IPs you'd
3 like to investigate.

4 For instance, if I was a law enforcement officer at a
10:55 5 university and I knew all of the University's IP addresses, I
6 could say just -- I want to investigate any of these IPs.

7 And with Torrential Downpour Receptor, if any computer
8 having that IP address comes to me offering to sell me drugs in
9 my analogy, or give me child pornography, then I would accept
10:55 10 that connection. I don't care about people in Russia or Spain
11 or France coming to my computer, I care about people in my
12 jurisdiction.

13 Or, the other possibility in the configuration, is I
14 specify by geographic region. And I think the Court's already
10:56 15 heard some of that through the defense expert. But it's
16 publicly available. You can go to lots of places on the
17 internet and you punch in an IP address and it will approximate
18 what city and state that that IP is being used in. And that's
19 just an effort for law enforcement to try to do investigations
10:56 20 in their primary jurisdiction and not poaching in someone
21 else's, so to speak.

22 Q. And so you reviewed the defense expert's affidavit.

23 A. Yes.

24 Q. And in there, in paragraph 24 essentially he asked what does
10:57 25 it mean to direct investigative focus. Is that what you're

1 saying, this program directs the investigative focus by saying I
2 want to do this in Wisconsin, or I want to do it in northeast
3 Wisconsin, or this particular series of IP addresses?

4 A. Yes. It's user configurable. And it does run -- I
10:57 5 configure it, I launch it, and it's set to investigate people in
6 Wisconsin. And it's ignoring all the other connection attempts
7 to us.

8 If I have a connection attempt from an IP address and
9 it approximates the location as being in Spain, I just refuse
10:58 10 that connection. I'm only accepting connections from the
11 Wisconsin area, if that's how I configured it. And that's how
12 you direct your investigative focus to a particular region, by
13 their IP addresses, or straight up with their IP address if I
14 knew that range off the [Indiscernible].

11:01 15 Q. And are those the settings that the investigator would be
16 able to essentially input?

17 A. That, a license, their name. Things of that nature. But
18 there is no setting that would enable them to -- enable a
19 feature that would be harmful or would make the software not
11:02 20 work properly.

21 Q. Or I want to go after this particular person or just white
22 males in a certain area, those aren't variables that this
23 program allows?

24 A. No, it's geographic region or IP address. And then you can
11:03 25 further restrict it. Although I'm sort of the gatekeeper as it

1 relates to what torrents do the systems seek out on the network.

2 I can't define what's illegal in every state in the
3 U.S., let alone every country in the world. I include torrents
4 to be investigated that presumably would have some violation
11:03 5 somewhere. It relates to child exploitation.

6 For instance, I could include pictures and movies of
7 17-year-olds engaged in sex, which is child pornography
8 federally and child pornography in Pennsylvania, where I'm from;
9 but in Connecticut, it's 16 or under.

11:04 10 So the onus is on the investigator to look at what's
11 downloaded and determine, yes, this violates our statute,
12 [Indiscernible]. But we don't just sit there and sniff and
13 listen to every piece of BitTorrent communication and try to
14 discern as the defense expert --

11:05 15 And, you know, obviously he hasn't seen the software,
16 but we aren't sitting there sniffing on the network or listening
17 and trying to discern this is child pornography and this is not.
18 No. We have the torrent. We're like every other BitTorrent
19 client. We reach out to the index, the matchmaker as I
11:05 20 described it earlier, and they provide us with IPs. That's it.

21 There's no listening for movie files, for anything
22 else; it's just the predesignated torrents in the system. We're
23 very refined. We're not searching for everything, we're looking
24 for a very specific subset of data.

11:06 25 Q. And to be clear, in this particular case Mr. Owens came to

1 law enforcement.

2 A. Correct. But let me just say that if he had come to law
3 enforcement and it wasn't one of the torrents we had chosen to
4 investigate, it would have ended there as well. Because we're
11:06 5 not going to talk to a person about it.

6 The other configuration I was leading towards -- and,
7 sorry, that was a little long-winded -- is that the end-user, if
8 they download material and they determine this is not violating
9 my statute in Connecticut, because it has to be under 16, they
11:07 10 have a mechanism to exclude those in future investigations. So
11 they can further refine it even more than the work that I've
12 done trying to identify the torrents leading to be investigated
13 by law enforcement.

14 Q. Okay. You had the opportunity to view the imaging of
11:08 15 Mr. Owens's computer I believe yesterday in my office, correct?

16 A. Yes.

17 Q. Okay. And I'll ask you what I asked the defense expert, did
18 you find any artifacts or evidence that this particular file had
19 been on Mr. Owens' computer?

11:08 20 A. Yes. The torrent which points to a file, yes, that both the
21 torrent and the file was on the system in -- excuse me -- in
22 three different areas.

23 Q. Okay. And did you print off basically information that
24 would reflect that that we can show to the Court and provide to
11:09 25 counsel?

1 A. Yes, I did.

2 MR. HUMBLE: May I approach, Your Honor?

3 THE COURT: You may, uh-huh.

4 BY MR. HUMBLE:

11:10 5 Q. I've handed you what have been marked Exhibits 4, 5 and 6.

6 Could you just identify those and tell the Court what they are?

7 A. Yes. These are just one portion of the forensic analysis.

8 4 relates to installed programs.

9 5 relates to torrent files.

11:11 10 6 relates to MRUs, or most recently used entries, from
11 the registry.

12 Q. Okay. And did you create these?

13 A. I created this printout, but the forensic -- it was part of
14 the forensic [Indiscernible].

11:11 15 Q. Sorry, that was imprecise. You created the images.

16 A. Yes.

17 Q. And that captures what you're trying to show here?

18 A. Yes.

19 Q. Okay. I'm going to switch those out, those duplicates, so
11:12 20 that the Court can follow along.

21 Now, I guess start with the first one which I believe
22 is No. 4?

23 A. Correct. So --

24 Q. Sorry. Could you just explain the significance of why
11:12 25 that's highlighted and what that reflects?

1 A. Yes. But before I get there, I just want to go back to this
2 log file where the computer that connected to the law
3 enforcement reported what software they were running. And they
4 reported it as being BitComet Version 1.50, which was
11:13 5 highlighted in yellow in those two exhibits we just went
6 through.

7 So the first thing I would look at would be to see if
8 there is a BitTorrent -- BitComet program installed, and sure
9 enough, BitComet Version 1.50 was installed. And
11:13 10 coincidentally, or not coincidentally, it was installed on May
11 20th at 9:07 -- I don't have my glasses on, I believe that's
12 right -- p.m.

13 So that's the date, the day before the investigation
14 happened. So the user of this computer installed BitComet
11:14 15 Version 1.50 the day before the investigation happened and was
16 memorialized in these logs. So that's the first -- that would
17 be Exhibit 4.

18 MR. DONOVAN: Your Honor, if I may, I would like to
19 interpose an objection. I think this is getting a little far
11:14 20 afield of the relevance of this hearing which is whether or not
21 we should have access to the program.

22 It sounds to me like he's trying to establish guilt
23 based on he had the program on this date, it was installed on a
24 certain date, then I guess there was, you know, torrents
11:15 25 downloaded.

1 It just seems like this is kind of far afield of where
2 we should be for today.

3 MR. HUMBLE: Except, Your Honor, that the defense
4 expert places great significance on the fact that he did not
11:16 5 find that particular file on the defendant's computer or in
6 multimedia. So I think it is certainly relevant that there was
7 strong evidence, which he also testified he did not find
8 necessarily, to show that this was there both before and after
9 law enforcement had any interaction with Mr. Owens's computer.

11:16 10 THE COURT: Overruled. And I assume we'll get to the
11 law enforcement privilege later. But this is kind of the
12 preliminary steps of how it works, as I understand it. And
13 it's -- I see this as testimony intended to show that the
14 defense is not in need of the software or the computer -- the
11:16 15 other materials sought. Now, that's arguable, I agree, and
16 certainly you'll be able to cross-examine and argue on that.
17 But at this point I think this testimony is relevant, so
18 overruled.

19 BY MR. HUMBLE:

11:17 20 Q. Okay. So, now, essentially he -- if this reflects that
21 [Indiscernible] the tool that was used to knock on law
22 enforcement's computer essentially and say I'm gonna give you
23 this, that's reflected on No. 4?

24 A. Correct. Because the file wasn't found, the next thing I
11:17 25 want to know as a forensic expert, okay, if it isn't there

1 today, deletion being a common thing we all do, let's show
2 whether or not it was there during the investigation, which is
3 what this was meant to do. So the software reported to law
4 enforcement was installed the day before the investigation took
11:18 5 place. That's the relevance of that exhibit.

6 Q. And how about Exhibit 5, what's the relevance of --

7 A. 5 is the torrent file named by its info hash. So if you
8 looked at the detailed log with the highlights that we went
9 through, remembering the first step is to agree that we're
11:18 10 talking about the same torrent file, that's step number 1.

11 Because if we can't agree that it's the same torrent, I'm done
12 talking to you.

13 If you look at the entry on Exhibit 5, the longest
14 cell, it starts "Partition 4 Microsoft NTFS." But if you look
11:20 15 at the next row down all the way to the end, you see a string of
16 numbers and letters, 0833, and then at the end it ends in 3C0, I
17 believe.

18 If you marry that up with the log, that's the exact
19 same info hash. So there's a date and time affixed to that.

11:21 20 May 20th at 9:29. So we're talking 22 minutes after he
21 installed BitComet -- he or she, the user of the computer --
22 20-some minutes later the torrent was downloaded and loaded into
23 BitComet. Why do I know that? Because the path of where that
24 torrent was found would only get there if you loaded the torrent
11:22 25 into the BitTorrent program. Otherwise it would just be sitting

1 in my downloads directory or on my desktop or someplace I chose
2 to save it. That's a hidden directory for applications to store
3 data they're using. So I know he downloaded the torrent and
4 loaded it into BitComet for it to be there.

11:22 5 Q. And what is the --

6 A. And that's the day before the investigation, to put it in
7 perspective, May 20th at 9:29 p.m.

8 Q. Okay. And the next exhibit, what is the significance of
9 that?

11:22 10 A. Well, this is most recently used. And when you touch files
11 and you access files, it will keep a record of that. And on May
12 22nd, a file with the exact same file name as the one sent from
13 the suspect computer to the law enforcement computer, is there.
14 And that's dated May 22nd at 1:38 a.m.

11:23 15 So the second investigation occurred on May 22nd at
16 3 a.m. So it's just an hours apart. It's still there so it's
17 being shared all the way from the 20th, when he started
18 downloading it, through the 22nd when the second undercover
19 session happened.

11:23 20 And I also note that in the exhibit where the torrent
21 was found, this -- there was more than one instance of him
22 having that torrent. There was one that dated all the way back
23 to January of 2016. And so what we are seeing more and more --
24 because I still do investigations beyond the development aspect
11:24 25 of my position -- more and more with the speed of the internet

1 and the efficiency of BitTorrent, not everyone keeps every file
2 they download. They download it, they look at it, and at some
3 point in time after that they delete it because it's so easy to
4 get it again.

11:24 5 And there's -- there's a reference to that same
6 torrent file all the way back to January of 2016. So that makes
7 me fall on the side of the fence that these files were getting
8 deleted as opposed to it was never there. It was clearly there.
9 That's what these forensic artifacts show.

11:25 10 Q. And correct me if I'm wrong, the log that we went through
11 previously, that's what law enforcement has -- receives,
12 correct?

13 A. Right. This is the memorialization of the events that took
14 place during the investigation made by Torrential Downpour
11:25 15 Receptor.

16 Q. And 4, 5, 6 were taken from the image -- the imaging of the
17 defendant's computer.

18 A. Yes, that's correct. That's a seized device.

19 Q. So these aren't married -- these are two opposite ends
11:25 20 essentially matching up.

21 A. Correct. Everything's lining up.

22 And I could have stopped just by reading this log.
23 There is no way that a computer at that IP address didn't
24 possess that data, to be able to give me 226 pieces that match
11:26 25 the right hash file. The computer had to be in possession of

1 that data to send it, and this just further confirms it.

2 Q. Okay. So let's get to law enforcement privilege then.

3 What's the harm in allowing testing to occur with
4 regard to Torrential Downpour Receptor?

11:27 5 A. Well, it has access. In order to run it you have to have a
6 license, first of all. That license is controlled by the system
7 I'm the administrator of.

8 And when you have a license to the software, it's
9 designed to download child pornography. And so you put in a
11:29 10 license and you specify an IP address or geographic region,
11 child pornography will be downloaded, because people will arrive
12 to our computer and offer to share child pornography with us.
13 So it exposes each and every torrent file we're investigating.

14 Again, to know the info hash of these torrents could
11:29 15 be harmful to law enforcement because if that gets out --
16 although, you know, people can promise never to release it, you
17 can't un-ring the bell. Once it's out it's done. We have to
18 start from scratch.

19 It's taken eight years to amass what we have here
11:29 20 today. At least eight. I can't remember the exact days when we
21 started, but it was at least eight years to get where we are
22 today.

23 It exposes the files we investigate and their hash
24 [Indiscernible].

11:30 25 It exposes law enforcement contact information of

1 investigators who are investigating individual IP addresses.

2 These are active investigation.

3 It exposes the IP address -- other IP addresses
4 associated with the torrents that we investigate. So, in other
11:30 5 words, these have yet to be investigated. There are just so
6 many people on BitTorrent sharing child pornography, we cannot
7 get to them all. I've trained personally hundreds, maybe
8 upwards towards a thousand investigators, and we can't come
9 close to getting all the people sharing child pornography on the
11:31 10 BitTorrent file sharing network. And I'm not even talking about
11 all the other areas that we can investigate.

12 So -- and finally, I mean, aspects of the system,
13 you're basically dropping a civilian in the mix of a raid
14 briefing. These are -- the system is designed to connect law
11:38 15 enforcement officers that have similar investigations based on
16 their IP addresses, they're in some stage of investigation, the
17 system alerts them of that, and you're dropping a civilian in
18 the middle of a raid briefing. If you're taking something
19 technology and trying to relate it to something real world, it
11:39 20 would be an equivalent.

21 Q. Were you saying raid, r-a-i-d briefing?

22 A. Raid like a search warrant.

23 Q. Okay.

24 A. Is what I was referring to.

11:39 25 Q. Okay. So, let me ask you, with regard -- in your opinion,

1 as someone who helped develop this program and obviously has a
2 lot of familiarity with it, is Torrential Downpour Receptor so
3 different from other BitTorrent programs that there is a strong
4 need for the defense to have this before they could
11:41 5 cross-examine somebody on the operations of this particular
6 BitTorrent?

7 A. The only point of confusion that I could see the defense
8 expert having, which he now has the answer to, was why a
9 computer would connect to us. He gave a definition of seeding.
11:41 10 And I don't know that he had a full understanding of what
11 seeding actually was.

12 But now with that question answered, this is -- this
13 is BitTorrent talk. This is not Torrential Downpour Receptor
14 talk. I mean, anyone should be able to look at this and see
11:42 15 that data was sent and it matches the corresponding hash
16 [Indiscernible]. The defense expert has the ability to look at
17 the torrent which is part of discovery, open it up and see all
18 of the hash values of all those 226 pieces, see that they were
19 verified, could even take the original file and hash those
11:44 20 individual segments to make sure that they do, in fact, belong
21 to that file, none of which requires our software.

22 This is -- this is a law enforcement BitTorrent piece
23 of software that, yes, employs the ability to download from a
24 single IP address as opposed to from multiples. Well, that's
11:45 25 law enforcement being more restrictive on itself.

1 I could get it really fast, but I'm willing to wait.
2 But it's not something unique to law enforcement software. A
3 download from a single sharing IP happen all the time.

4 So I don't believe that there is a need to confirm it
11:45 5 when we've detailed it as specifically as we have. This is all
6 information, as the defense expert said, that any BitTorrent
7 client would know. But whether or not it chooses to display it
8 to the user, and certainly probably wouldn't memorialize it to a
9 log file like this, but it is to aid the prosecution, but it's
11:46 10 also letting the defense expert know exactly what happened at
11 what moment in time.

12 And he can confirm these things through the forensic
13 analysis, as I did. I spent 10 or 15 minutes and found these
14 three items. There's probably much more on there that I didn't
11:46 15 look at, and to have the torrent file and the data, that should
16 be sufficient.

17 Q. In your expert opinion, if there had been a bug or a glitch
18 in the software, would that be reflected in the things that
19 you've reviewed prior to your testimony here today?

11:47 20 A. Yes. I mean, I would get the bug reports. I would know if
21 there was a bug report. If people are continually downloading
22 files and they didn't come from the sharing computer, I would
23 know to seek that out.

24 But it's a very simple process. As the defense expert
11:47 25 said, the IP addresses have a source and destination IP right in

1 every packet of data. It's not hard to discern where it came
2 from. And we just memorialize that in this document.

3 And, again, that IP address came to us. Just like if
4 you visit a web page, that web server knows your IP address
11:48 5 immediately. Well, the suspect computer came to us. We
6 documented the IP address, we allowed the communication to
7 happen, and then we received the data they wanted to share with
8 us.

9 Q. Would you -- based on your knowledge of Torrential Downpour
11:48 10 Receptor, would you describe it as bug-ridden or buggy as I
11 guess software people say?

12 A. No. Early on in its early stages of development we had the
13 source code looked at, and there was one issue -- and this is
14 eight years ago -- where we weren't accounting for long file
11:49 15 names that exceeded 260 -- or the path and file name to exceed
16 260 characters, that was fixed, and that was the end of the bugs
17 as it relates to downloading.

18 BitTorrent is a very, very light-weight small
19 protocol. A BitTorrent program like BitTorrent or uTorrent are
11:50 20 like a couple megabytes. It's the size of a single picture.
21 It's not a ton of code that could be bug-ridden like the defense
22 expert's example of an operating system or Microsoft Word that
23 are millions of lines of codes. We're talking about 2 megabytes
24 of programming.

11:50 25 So, but that was fixed eight or more years ago, the

1 long file name issue, and all that would have done was shut the
2 program down. It wouldn't have collected erroneous information.

3 And the fact that BitTorrent relies on SHA-1 hashing,
4 which is extremely accurate, you're not going to get the false
11:52 5 positives because we're confirming the data through hashing, the
6 same thing forensic examiners use to confirm I'm working from an
7 exact duplicate of the hard drive seized. We rely on it day in
8 and day out. Well, BitTorrent does as well. And through
9 hashing, short of SHA-1 hashing failing, which is very, very
11:52 10 accurate, you're not going to get a [Indiscernible] false
11 positive.

12 MR. HUMBLE: Judge, I don't have any further
13 questions.

14 THE COURT: Mr. Donovan?

11:53 15 MR. HUMBLE: Could I just ask that those exhibits be
16 received, Your Honor?

17 THE COURT: 1 through 6 received.

18 I take it there's no objection.

19 MR. DONOVAN: Well, Your Honor, I mean, we didn't see
11:53 20 Exhibits 4, 5 and 6 before today, but, I mean, no objection as
21 far as --

22 THE COURT: I don't think they existed before today.
23 It sounds like they were run off today. Is that right, Mr. --

24 MR. HUMBLE: Was it this morning or last night? Last
11:54 25 night perhaps.

1 THE WITNESS: To be clear, this is the forensic report
2 of the forensic examiner. This is the material that was --

3 MR. HUMBLE: Yeah, it's been provided, just not the
4 exhibit --

11:54 5 THE COURT: Okay.

6 MR. DONOVAN: Your Honor, we don't deny that the
7 forensic material was provided, but, I mean, it's large. It's
8 very voluminous. And we did not see these exact references
9 until today.

11:54 10 THE COURT: Yeah. But you had access to the hard
11 drive or the computer --

12 MR. DONOVAN: Correct, yes.

13 THE COURT: -- evidence from which this was taken.

14 I'll overrule the objection and 1 through 6 are
11:55 15 received.

16 (Exhibits 1-6 received in evidence.)

17 MR. DONOVAN: Thank you.

18 CROSS-EXAMINATION

19 BY MR. DONOVAN:

11:57 20 Q. Good afternoon. Getting towards the evening here shortly.

21 Okay. So you have testified that you were part of the
22 original development for all of these types of programs,
23 correct?

24 A. Yes.

11:57 25 Q. And it's been kind of an evolution from probably -- I don't

1 know if Gnutella was maybe the first iteration all the way up
2 through now BitTorrent. Right?

3 A. There are many file-sharing networks that we have
4 investigative tools for.

11:59 5 Q. Can you I guess more precisely describe your role? Because
6 you said you didn't do any of the actual programming, correct?

7 A. I didn't write Torrential Downpour Receptor, the program
8 being used. I did programming on the back end and testing of
9 the software. But with the other tools there are programming
11:59 10 elements that I did participate in, it's just not with
11 Torrential Downpour Receptor. The physical program sitting on
12 the investigator's computer, how it logged search results and
13 things like that I was involved.

14 Q. Okay. How long did the development take of Torrential
11:59 15 Downpour?

16 A. From the point in time where we first talked about it at the
17 University of Massachusetts to releasing the first version, it
18 was well over a year. Maybe more.

19 Q. And maybe this is a good time, can you explain the
12:00 20 difference between Torrential Downpour and Torrential Downpour
21 Receptor?

22 A. Torrential Downpour wasn't used in this case and it doesn't
23 sit and wait for suspect computers to arrive to our computer.
24 It's the complete opposite of that.

12:00 25 So Receptor sits and listens passively for people

1 coming and knocking on our door asking to share torrents that we
2 know that involve child exploitative material.

3 Torrential Downpour makes outbound connections trying
4 to connect to somebody that may or may not be sharing child
12:01 5 pornography.

6 That's the big difference. We sit passively and wait
7 for the suspect to come to us.

8 Q. Is the only way you know which one was used in this case is
9 from reviewing the logs? Or did you talk directly to the law
12:01 10 enforcement officers who ran this?

11 A. Well, the log certainly tells us -- that's the whole purpose
12 of putting on the first line the software that's used. But
13 beyond that, through networking I can tell that.

14 In the extended handshake he tells us what his listing
12:02 15 port is. So if I were to connect to him, I would connect into
16 that port. I know we're getting kind of technical. But you can
17 see at the top, he connected to us because it's an outbound
18 port. There's a specific range of ports. Of the 65,000
19 ports -- there's more than 65,000 ports available to use --
12:02 20 there's a set of ports set aside just for making outbound
21 connections.

22 So it's proof that the suspect computer connected to
23 us. The networking ports alone tell you that. And the software
24 that we indicate we were using at the top of the log indicate
12:03 25 that. That's the only functionality it has, is to receive an

1 inbound connection which triggers an investigation.

2 Q. But, again, you would agree that the logs are a subset of
3 the program, correct?

4 A. The --

12:03 5 Q. They're generated by the program.

6 A. They're generated by the program, I agree with that.

7 Q. And so the information that comes from the program dictates
8 what's on the logs.

9 A. Correct.

12:03 10 Q. In other words, the logs aren't an independent check or
11 verification of anything, it's a subset of the program that
12 we're talking about.

13 A. Correct. The computer comes to us, we see the IP address,
14 we memorialize it in the log. Correct. Which is Windows,
12:04 15 actually.

16 Q. What language is Torrential Downpour Receptor written in?

17 A. C#.

18 Q. Okay. And so obviously this involved, you know, computer
19 scientists and software developers and other people besides
12:06 20 yourself to put it together, correct?

21 A. Me and one guy, Brian Lang.

22 Q. Okay. Oh, just the two of you.

23 A. Yes. And it's not -- it was written by the ground up from
24 the university. It was not a modified version of an existing

12:07 25 program. So that was incorrect information the Court had heard.

1 It was written by the University of Massachusetts Amherst. And
2 the team of developers beyond the initial research is me and
3 that one individual.

12:08 4 Q. Okay. Now, you've reviewed the pleadings in this case,
5 right?

6 A. Yes. Well, I've read the defense expert's report/affidavit.

7 Q. Did you read any of the motions filed by either me or the
8 government?

9 A. I did not. They were already filed and done before I even
12:08 10 had communicated with the office. I don't believe I -- I did
11 have a copy of the police officers' report. I never had a copy
12 of the search warrant. And then obviously I have the two
13 detailed logs.

14 Q. So, sir, are you aware that the government has said that
12:08 15 basically the investigator in this case accessed BitTorrent like
16 a normal or average user of the program? I'm talking about the
17 normal BitTorrent program, not the law enforcement program.

18 A. Can you repeat that? I don't want to --

19 Q. Are you aware that the government's characterized law
12:09 20 enforcement's use of BitTorrent here as a normal or average
21 user?

22 A. I am now, I wasn't before. But I don't feel that that's
23 inaccurate.

24 Q. You don't feel that's inaccurate.

12:09 25 A. No, we follow the protocol. And just like any other program

1 can receive an inbound connection and download any or all of
2 that data, we did the exact same thing except we memorialize the
3 data and we don't share.

4 Q. Well, there's -- I mean, there's a lot of other things that
12:10 5 the program does the public version doesn't, right?

6 A. (No response.)

7 Q. And I can give examples.

8 A. Okay.

9 Q. Would you agree that, again, it does single source
12:10 10 downloads?

11 A. Correct. The general public does that as well.

12 Q. And I understand you testified that that could also happen
13 in the public if there was only one computer sharing this one
14 file that could be a single source, but your program doesn't
12:11 15 even when there's multiple sources available which would be
16 contrary to the normal protocol, right?

17 A. Our program I'm sure it happens every time, but it happens
18 naturally every day on the internet.

19 Q. But yours insures it only happens on single source
12:12 20 downloads.

21 A. Right.

22 Q. Right? It wouldn't do any good to get multi-source
23 downloads and then try to figure out who to attribute this to,
24 right?

12:12 25 A. That would be counterproductive. It would add a burden to

1 law enforcement.

2 Q. And your program -- and I think you testified earlier that
3 it doesn't fake file share, it just says it has no pieces to
4 share, right?

01:09 5 A. Because we have no pieces to share we appropriately say we
6 have no pieces to share.

7 Because the computer -- since we're employing a single
8 source download, every piece of data we have received came from
9 the computer that connected to us. So there is no need for us
01:09 10 to ever share any data back because everything we have came from
11 the sharing computer.

12 Q. Well, I understand, too, you don't want to share contraband,
13 correct?

14 A. Correct.

01:10 15 Q. Okay. How do you then -- so the program does something to
16 stay on the BitTorrent network and not get kicked off, right?

17 A. That doesn't exist. And I don't -- I'm not sure what the
18 defense expert was talking about.

19 Q. Well, have you heard the term "throttling" before?

01:10 20 A. Yes, you can throttle. That's not being kicked off the
21 network.

22 Q. Oh.

23 A. So, in other words, there are incentives. If you share, if
24 you employ that tit-for-tat exchange, so I'm giving pieces as
01:11 25 I'm getting pieces, you're -- the allocated bandwidth you're

1 given is increased. So I might get that file a little quicker.

2 But, to not share, I'm still able to download and I'm
3 not kicked off the network and I'm not fake file sharing.

4 Q. Okay. I'm sorry, I don't mean to be imprecise. I didn't
01:11 5 mean to say kicked off the network. But you could get throttled
6 if you're not sharing, right?

7 A. You could receive your downloads slower than other
8 BitTorrent clients.

9 Q. But here you testified that based on the logs these
01:12 10 downloads actually occurred pretty quickly.

11 A. Correct. Because the client didn't need any pieces for us.
12 The tit-for-tat exchange was gone. That, on top of the fact it
13 was an AT&T U-verse connection, which has a large amount of
14 upload bandwidth which is the one exception. AT&T U-verse and
01:12 15 Verizon Fios have huge upstream bandwidths. So what the defense
16 expert was describing really doesn't apply because the
17 connections are so fast. But it's only a 15-megabyte movie, so
18 I expect it to happen fairly quickly with the speed of the
19 internet today.

01:13 20 Q. So just to be clear, is your testimony that the program does
21 not do anything to stay on the network that an average user
22 couldn't do? To avoid being throttled or --

23 A. I don't even understand what you mean by on the network.
24 Because you're on the network every time you load a torrent file
01:14 25 into your program. You don't get kicked off. A user can choose

1 to share the data with you slower. And, yes, that is part of
2 the incentive scheme for this give-to-get scenario on
3 BitTorrent. But it doesn't preclude you from getting everything
4 without sharing one single bit of data, which happens naturally
01:14 5 every day on the network.

6 Q. So does Torrential Downpour do anything to avoid throttling?
7 I shouldn't say kicked off. Avoid throttling for not sharing.

8 A. No. We properly say we have nothing to share at the
9 beginning of the session. And then if ever we're asked again,
01:14 10 if we handshake again, which happens sometimes, we would report
11 what pieces we did have to share.

12 Again, the sharing client gave us every piece we
13 possess. There is no need for him to ever request that back
14 from us. So this whole tit-for-tat exchange and the throttling,
01:15 15 as you put it, of the bandwidth doesn't really come into play in
16 this case specifically because they were seeding. They had all
17 of the content. There is no need to throttle data. Its purpose
18 in life when it's seeding is sharing the data proactively out to
19 the network to keep that data alive on the BitTorrent network.

01:15 20 So throttling really isn't in play when there's a seed.

21 Q. Is it ever in play, though? I mean, it's not in play in
22 this case, but can it ever be in play that you get throttled?

23 A. Oh, absolutely. Again, if I never share a piece of data,
24 which we don't, I will never benefit from added bandwidth from
01:16 25 the sharing client.

1 Additionally, clients at times, depending on --
2 there's so many variables to go into, but depending on how
3 popular the torrent is, they could actually share with me for a
4 period of time and then disconnect from me. And then later, as
01:17 5 any BitTorrent client would, you can reconnect and ask for
6 additional pieces. Again, I'm in the same situation.

7 Q. So I'm not trying to belabor this, but, again, not in this
8 case, but does Torrential Downpour Receptor ever do anything to
9 not get throttled in general to be able to keep up fast --

01:17 10 A. No.

11 Q. -- and do what it wants to do?

12 A. To the contrary. We get throttled is what I'm trying to
13 say. We didn't here because --

14 Q. Okay.

01:17 15 A. -- he was seeding. But there is no secret mechanism to keep
16 us getting data faster than we deserve to get it. It doesn't
17 exist. And I wasn't trying to avoid the answer --

18 Q. Okay. It's fine. I apologize. I probably wasn't being
19 precise enough.

01:18 20 Torrential Downpour Receptor again generates these
21 specialized data logs that you've talked about which the normal
22 program doesn't do, correct?

23 A. Correct.

24 Q. Okay.

01:18 25 A. It's information known by the programs, but there would be

1 no purpose for BitComet to write out a log like this.

2 Q. And it conducts searches against the hash library, you've
3 talked about, right?

4 A. (No response.)

01:19 5 Q. Again -- in other words, you have a set of hash values that
6 you are looking for torrents that report having an association
7 with them, correct?

8 A. Correct. We're searching for a torrent exactly like any
9 other program out there. As soon as a torrent gets loaded into
01:19 10 BitComet, which is the program in question here, it actually
11 searches for download candidates.

12 And that's what we do. We physically load a torrent
13 into Torrential Downpour Receptor, and then it searches the
14 network for download candidates. It's exactly the same.

01:20 15 Q. Now, to be clear -- to be clear, when you say "we" it's
16 actually you. You maintain control exclusively of the database,
17 or library, whatever you want to call it, of all these hash
18 values you're looking for, right?

19 A. What torrents we search for I'm in control over. What is
01:20 20 being searched for by the investigator is an actual torrent file
21 being loaded into Torrential Downpour Receptor like any other
22 program. We're just excluding the commercial movies and the
23 commercial music and the illegal, you know, copyrighted programs
24 that are traded on BitTorrent and we're only focusing on child
01:21 25 exploitation material.

1 Q. Again, that you decide on, correct?

2 A. I decide on what is to be searched for. The investigator
3 decides on what to use as probable cause for a charge.

4 Q. Okay.

01:21 5 A. And they make suggestions. They will submit torrents to me
6 to be evaluated to be included into our system.

7 Q. Can you describe a little bit about how the program is set
8 up by someone who's got a license and is trained to do this?

9 A. Sure. It has an installer file just like any other program.
01:21 10 You double-click an installer file. It will ask you some
11 questions. Some questions already have answers to them. But it
12 will ask you to input your name. There are options to put in
13 your email address. But you have to have a license number to
14 run it or else it won't function.

01:22 15 So we control who has a license. So if the software
16 gets out there it's nonfunctional without the license, it will
17 do nothing.

18 You will specify with Receptor what geographic region
19 you'd like to investigate. Or you could express it by the
01:22 20 physical IP address or a range of IP addresses, which is the
21 trigger to the program to decide whether to, as the investigator
22 put I think, direct his investigative focus towards a particular
23 IP or not. It's based on his settings. He's told the computer
24 investigate these IPs or just investigate people in Wisconsin as
01:23 25 opposed to anywhere in the world.

1 And there are settings regarding how long should we
2 wait for the download to complete. Because we're not gonna wait
3 forever. And so we can just stop the investigation after a
4 predetermined period of time. The default I think is four
01:24 5 hours.

6 Q. And this program can run automatically, right, after it's
7 set up and configured?

8 A. Correct. You're going to configure it and set it up and
9 it's going to search for torrents and receive those inbound
01:24 10 connections automatically. The logs get written out
11 automatically as well.

12 Q. So does the investigator typically just check the results
13 like every day, every week, every month? Like how does that
14 work?

01:24 15 A. Well, I can't speak for every investigator, but on every
16 shift of my work I check my logs.

17 Q. Okay. Okay. So going back to the logs that have been
18 introduced as Exhibits -- I believe 2 and 3, how do those logs,
19 for example, like establish by themselves that Torrential
01:25 20 Downpour Receptor doesn't invade, for example, the shared space
21 of a computer?

22 A. Well, it basically comes down to -- well, first the suspect
23 computer comes to [Indiscernible]. That's the first piece.

24 The second piece is just to understand BitTorrent, if
01:25 25 you understand the BitTorrent set of rules that have to be

1 followed and how it functions, it's -- what you're describing is
2 impossible.

3 I can't -- if I wanted to download -- excuse me, I'm
4 sorry.

01:25 5 If I wanted to download a file from some unshared
6 location on the computer, I can't even do that because both the
7 sharing computer and the investigating computer -- or in another
8 way I could say that as any two BitTorrent programs -- would
9 require that you have the exact same torrent file.

01:26 10 I can't -- there's no function within BitComet, which
11 is what was used on the suspect computer in this case, there is
12 no ability to download anything. We can only receive what the
13 sharing computer permits us to get.

14 Q. So is your answer that the program just can't do it and,
01:27 15 therefore, that's why it's not on the logs? Is that --

16 A. It's -- yeah. Not even BitComet. Any BitTorrent program on
17 this planet require a torrent file on both sides with that
18 really unique identifier. I have no way to know where these
19 files are on the suspect computer, let alone create a torrent
01:28 20 file, load it into his BitTorrent program, just so that I could
21 then investigate him with our BitTorrent software. There's just
22 no mechanism. You'd have to show that there was a flaw in
23 BitComet at Version 1.50 that allowed some crazy intrusion like
24 you're describing, but that doesn't exist.

01:29 25 Q. Are there any other types of logs generated besides what's

1 been entered as exhibits or is that the comprehensive log?

2 A. This is the comprehensive log. There's also a net -- a
3 netstat. Because for reasons just like this, there's a Windows
4 program that will record TCP connections.

01:29 5 And earlier as I was describing how the suspect
6 computer connected to the law enforcement computer, it was
7 through something called a TCP connection. And Windows has a
8 utility that will track all of the TCP connections between my
9 computer and other computers. So we run this netstat program,
01:30 10 this windows program that has nothing to do with us and our
11 development, to confirm, to give corroborative evidence that,
12 yes, this other program came to the same conclusion as us that
13 there was an active TCP connection between us and the suspect
14 computer.

01:31 15 So there's the netstat log. There's a summary log
16 which is just less verbose than the detailed log. There is the
17 torrent info.txt file which gives you all of the information
18 inside of the torrent that is used to calculate that unique
19 identifier, that info hash I spoke of.

01:32 20 There's two XML files that contain data and I don't
21 remember them off -- the names off the top of my head. Those
22 XML files are just data that help us evaluate the case more
23 quickly.

24 It's the same data that you're finding in the detailed
01:32 25 log in other areas. We have a program that helps us parse

1 through that and realize information. So that's what those XML
2 files are for. And then you have the actual downloaded material
3 which is in a download directory.

4 So that's the output of the software, all those items.

01:33 5 Q. Are there any other either libraries or software packages
6 that the program relies upon or uses?

7 A. No. Actually there's no libraries. Everything was written
8 from the ground up. There was a point in time I think he was
9 using an open source library, but he ceased using that years
01:34 10 ago.

11 Q. So is it like -- I mean, I'm not trying to be too basic
12 here, but is it literally like one file, the program? Like one
13 application file? Or does it have associated files with it?

14 A. Yeah. I mean, you're gonna install a program and it's one
01:34 15 file to start the installation, but it's just not a single file
16 that makes it work. There's configuration files and such.

17 For instance, when you're inputting the settings on
18 who you want to investigate, that has to be stored somewhere.
19 There's other associated files [Indiscernible].

01:35 20 Q. Okay. Is Torrential Downpour Receptor actively maintained?

21 A. Yes. It's worked on and maintained by the University, who
22 is the owner of the software. It still exists. And, you know,
23 there may be features we want added to it. That programmer is
24 still available to accommodate law enforcement requests.

01:36 25 Q. How about like, are there patches done to it occasionally?

1 A. Oh, there's new versions released to implement new features
2 that we want to make law enforcement's job easier in evaluating
3 the case. There's so many people on BitTorrent sharing child
4 pornography that we want to try to get the most egregious stuff
01:37 5 first. Those are the changes that are being made in the new
6 release.

7 Q. Is it your testimony that there's really only been one bug
8 with this program since the time it was developed?

9 A. That's the only bug that I know of that relates to single
01:37 10 source downloading, and it was reviewed -- it was the long file
11 names, which was handled.

12 Q. Who found that or who reviewed that?

13 A. Before the FBI would let the -- their agents use the
14 software, which we had already bought through a grant, and they
01:38 15 did an independent validation of the method in which we do
16 single source downloading to confirm that we don't share, which
17 obviously law enforcement can't become part of the problem, and
18 that it does employ properly as [Indiscernible].

19 Q. I don't know suppose that FBI validation is publicly
01:39 20 available.

21 A. No. I mean, the purpose of them doing it was to permit the
22 agents to use the software we developed. And now they've
23 abandoned their own programs and just use the whole
24 [Indiscernible] that make --

01:40 25 Q. But again, that's not something that we can look at, that

1 validation.

2 A. I don't have it. I've read it once, and that's why I know
3 that was the bug that was seen and fixed immediately. And,
4 again, I'm the administrator of the entire system still to this
01:41 5 day. It's housed by the Pennsylvania State Police in a computer
6 center and I would receive those bug reports. I don't know of
7 any other bug that would affect [Indiscernible].

8 Q. So you're the only person that would get reported to if
9 there was a problem?

01:41 10 A. Me or the developer. If any other instructor would receive
11 it, it has to come to me eventually, or the programmer.

12 Q. So how often typically is it updated?

13 A. The version that's current -- I don't think there was any
14 release in the last six, eight, ten months maybe. There may be
01:42 15 some years where there were a couple releases. Because we,
16 again, they're feature enhancements, not changing the method in
17 which we single source download. But we may want to be able to
18 flag the most egregious torrent as opposed to torrents that have
19 pictures of kids modeling adult lingerie or something like that.

01:42 20 Q. Well, that would just be more updating the hash database,
21 right?

22 A. No, that's updating the program and how you look at it.

23 Q. Okay.

24 A. How you look at the data.

01:43 25 Q. What type of network connectivity does it require?

1 A. It uses TCP communication for the file transfers.

2 TCP, Your Honor, is transmission control protocol.

3 And it's, again, that type of internet traffic that I compared
4 to like a phone call. You dial a number, you say hello, hello.

01:43 5 There's error correction, all kinds of things.

6 Some of the indexing that BitTorrent uses also uses
7 UDP packets, which are connectionless packets. And that's for
8 once you load the torrent, so that you can get those IPs of
9 people associated with the torrent. That comes via UDP

01:44 10 depending on which index you're connecting to. So it uses both
11 TCP and UDP networking.

12 Q. Do you test to determine whether it's operating correctly
13 from time to time?

14 A. Yes. You test it at the conclusion of every class with the
01:44 15 students. I test it before the release of the software.
16 There's a validation process.

17 Q. So you've done that testing in the past. You say you do it
18 every class that you teach?

19 A. Yeah, at the conclusion of the class we go through a
01:44 20 process. Because it's automated the end-user in the class,
21 we'll go through a validation process.

22 So, for instance, if we're gonna rely upon a log as
23 the basis to get a subpoena for a subscriber or eventually a
24 search warrant, then that investigator needs to trust that the
01:45 25 logs' dates and times are correct.

1 So we have a computer that's sharing content and a
2 computer that is investigating. And we show both screens. And
3 as -- as events happened we confirm that the dates and times in
4 the log are correct. We confirm that the IP address purported
03:11 5 in the log is correct. Because we're controlling both sides of
6 the communication, so we know the sharing computer's IP and the
7 investigating computer's IP.

8 We verify that it properly weights out the info hash
9 of the torrent in question, and that it dates and timestamps
03:12 10 appropriately throughout that log.

11 And then, finally, it calculates the MD5 and SHA-1
12 hash at the conclusion of the transfer.

13 Q. So in this training or this validation testing you just
14 described, you're controlling both computers, correct?

03:13 15 A. Correct.

16 Q. Are you actually transferring child pornography or is it
17 just a benign file of something else?

18 A. It's a benign file.

19 Q. So why couldn't that be done for the defense?

03:13 20 A. Well, it exposes all those other things to our system.

21 Again, once you have a license to our software, you
22 see active investigations, you see contact information for the
23 investigators, you would learn all of our hash values, all the
24 info hashes of the torrents. But it is possible to set up a
03:14 25 torrent with data that is not child pornographic, but it takes

1 my involvement.

2 Q. Well, in fact, so you've done that before for the defense
3 counsel, right?

4 A. Done what?

03:14 5 Q. A demonstration or a validation testing.

6 A. I've done demonstrations. But when I do demonstrations I
7 can just actually -- I can actually just transfer child
8 pornography. In my test I run the system, I actually download
9 [Indiscernible] log. I don't have to show them the movie file
03:15 10 that gets downloaded. But additionally, we have offered a
11 validation test -- although it's in-house, we've offered a
12 validation test I think for [Indiscernible].

13 Q. So you have offered some access before to defense counsel,
14 right?

03:16 15 A. Not to the software. A validation test which is documented.

16 The whole process, like I describe to our students,
17 we'll test the software so they can be comfortable with the
18 dates and times, the logs, what's logged. There's a whole
19 validation process. And just like the students would see, both
03:18 20 the sharing computer and the investigating computer, we do that
21 with video screen recording. So visually you can see that the
22 software is connected to the sharing computer. The logs are
23 shown. And so you can verify the dates and times are accurate.
24 And then, finally, there's a packet capture.

03:18 25 As the defense brought out, that can be used to prove

1 single source downloading, which is the only thing that I saw
2 other than the questions he had in his report was more of a
3 what-if scenario, what if it was downloaded from someone else.

03:19 4 So that's the only thing I really saw in his report
5 that was any question as to the reliability of our software
6 short of not finding a file, but clearly it was there.

7 So that packet capture is proof of single source
8 downloading as your own expert said.

03:20 9 Q. But you've never let anybody do a packet capture, you never
10 let anyone have hands on the program. The most you've ever done
11 is let them just watch your demonstration controlled on both
12 ends from you.

13 A. Correct.

14 Q. Or by you.

03:20 15 A. It's documented in such a way it couldn't be altered. Hash
16 values of all the elements of the tests are recorded and seen
17 visually and memorialized [Indiscernible].

18 Q. Has the government asked you to be able to do that here
19 today, you know, in this case?

03:21 20 A. No, the government never -- again, I got involved in this
21 case I think after the motion -- the pending responses or
22 motions were filed. It's only been a couple weeks that I've
23 been involved in the case.

03:22 24 Q. All right. So when you do a single source download from the
25 IP address that you identify as a target computer, okay? Do you

1 know how long at that point that the source computer had that
2 file?

3 A. No. If you had search results, a history recorded, you
4 could have an idea of about how long. But normal BitTorrent
03:22 5 communication, no, would not tell you that.

6 Q. And you didn't know -- you wouldn't know where they got it
7 from, where the source computer might have gotten it from in the
8 first place, right?

9 A. No. No. I mean, that's true with file sharing as a
03:23 10 whole --

11 Q. Okay.

12 A. -- across the board, yeah.

13 Q. So it could have been downloaded by that source computer as
14 a single file or it could have been downloaded in a batch. I
03:23 15 think you testified earlier that you can download, you know,
16 multiple files at one time, right?

17 A. Yes. Some torrents describe one file, as it was in this
18 case, or it could be dozens or more.

19 Q. So it could be a situation where a user of a computer is
03:26 20 downloading dozens of files, a whole batch of files and, you
21 know, maybe one of it or some of it's child pornography, the
22 rest is legal material.

23 A. That's certainly possible. That's the whole purpose --
24 that's why we get search warrants and do an interview.

25 Q. Right.

1 A. Because we'll never know that before the search warrant
2 and -- we're dealing with the internet here.

3 Q. So I think you testified earlier -- so you say that it
4 doesn't sniff data across the network in total, but you must be
03:32 5 doing some sort of narrowing-down or winnowing process that only
6 gets you what you're looking for which means by definition
7 you're excluding other things, right?

8 A. No. I have a torrent. Although I'm the gatekeeper of all
9 the torrents, each investigator has a physical torrent. They
03:32 10 load it into a physical BitTorrent program, Torrential Downpour
11 Receptor. It searches for download candidates and then it
12 receives search results.

13 Done. That's it. But that's every BitTorrent client.
14 That's different than saying like with a wiretap, a phone
03:33 15 wiretap, you're listening to all conversations in and out. With
16 a packet capture, as the defense expert described, that's
17 listening to all the communication on a wire.

18 Here we are searching, issuing a search request to
19 find IPs and receiving results and recording it. That's it.
03:33 20 It's not like we're listening on the internet for any time any
21 BitTorrent communication happens and I can somehow magically
22 discern one from the other. That's not at all what happens. We
23 just search and receive results. That's it.

24 MR. DONOVAN: Your Honor, if I could have one minute
03:38 25 to consult with my expert.

1 (Brief pause.)

2 MR. DONOVAN: Your Honor, I don't have any further
3 questions.

4 THE COURT: Mr. Humble, anything else?

03:38 5 MR. HUMBLE: No, Your Honor.

6 EXAMINATION

7 BY THE COURT:

8 Q. Mr. Erdely, you said that one of the concerns about allowing
9 an expert to share or look at some of these things is that it
03:38 10 would expose hash values?

11 A. Correct. It would expose -- it's taken years to amass the
12 instruction files, those torrent files that law enforcement are
13 seeking out. If any of that --

14 Q. Aren't those -- I thought those were publicly available.

03:39 15 A. They are publicly available. They're not -- but what the
16 public doesn't know is what areas we, law enforcement, exist in.
17 We're looking for these 500,000, 2,000 torrents. To put that
18 out there would give them the key to not get caught. We'd have
19 to start from scratch.

03:39 20 Q. Okay. So you don't want them to know what you're looking
21 for.

22 A. Correct.

23 Q. The other thing is, now, Exhibits 2 and 3, the logs, are
24 essentially downloads of the exact same video?

03:39 25 A. Yes, sir. That computer was online sharing it over two

1 days.

2 Q. Why -- I thought -- you know, if you put out the request,
3 why does it pull in from the same person twice?

4 A. And actually you can -- there are settings to avoid that.

03:40 5 If you downloaded the whole torrent from somebody --

6 Q. Yeah.

7 A. -- in our software you can say don't try to download again.

8 But, I believe your question is more about why would -- why
9 would the same computer come to us to be overly helpful and

03:46 10 share the whole file with us the second time when they had just
11 done it the day before. Is that summarizing --

12 Q. Yes. And your initial log says we don't have any of it.

13 A. Right.

14 Q. But by that time, the time the second download happens, you
03:47 15 have it all.

16 A. Right. But that's a whole other investigative session. So,
17 to remember, and we haven't really talked about it in this
18 hearing much, IPs are dynamic. They change. I could have one
19 IP address today and another IP address tomorrow. There is
03:47 20 nothing that is going to enable me to know, even though it's the
21 same IP address, a day later. I don't know for certain it's the
22 same individual.

23 Q. Okay.

24 A. They're dynamic and can change daily or even hourly.

03:48 25 Q. Now, we just have the logs that came from the IP address of

1 the defendant. In this same investigative session is it likely
2 that this search or this -- not so much a search, but they
3 received -- after inputting this torrent, this hash value --
4 received a number of other hits as well where there were other
03:48 5 individuals now that they followed up on?

6 A. Yes. So the software isn't going to just sit there and
7 investigate one person at a time.

8 Q. Right.

9 A. There are different programming threads that you could have
03:48 10 multiple investigations going on at any given time. So, for
11 instance, I could have through my web browser five tabs open
12 with five different web pages.

13 Q. Uh-huh.

14 A. But tab 5 doesn't somehow get mixed up with tab 1. I see
03:49 15 MSN here, I see CNN there.

16 Same concept. And Windows controls that. It's not
17 even -- if there was an error in that, you would need to go to
18 Microsoft and say why aren't you controlling your TCP
19 connection.

03:49 20 Q. Yeah.

21 A. But it's separate tunnels, so to speak, separate TCP
22 connections, so one would never get mixed up with another one or
23 Windows is failing.

24 Q. And then lastly, I think you've covered this, but you said
03:50 25 you had that bug maybe eight years ago or whatever and the

1 result of it was it just didn't work. It wasn't that it gave
2 false information, it just doesn't work. Is that --

3 A. Right. It would just cause the program to stop working
4 because -- to put it in context, Windows allows for, you know,
03:50 5 the folder, all the folders and sub folders and the file name
6 can't exceed 260 characters.

7 Q. Uh-huh.

8 A. So the programmer said, okay, we're gonna limit it to 260
9 characters. That's what Windows says. But the problem is other
03:50 10 operating systems like a UNIX or Linux environment or Mac can
11 have even longer extensions, so we had to account for that.

12 So programmatically they're accounting for the fact
13 that some of these paths and file names could exceed 260, which
14 doesn't make Windows happy, but we had to account for it because
03:51 15 BitTorrent is not just unique to a Windows computer, it runs on
16 Mac and Linux and all these other operating systems.

17 But that was the extent of the bug. And you're right,
18 Your Honor, it would just shut the program down. It didn't
19 collect false information or give us false negatives or
03:51 20 positives, it just shut down. So that's a case I will never
21 investigate.

22 THE COURT: Okay. Any follow-up?

23 MR. HUMBLE: No, Your Honor.

24 THE COURT: All right.

03:54 25 MR. DONOVAN: I do have just a little follow-up based

1 on some of these questions and answers. And I appreciate it,
2 Your Honor.

3 FURTHER CROSS-EXAMINATION

4 BY MR. DONOVAN:

03:54 5 Q. You would agree that an info hash is different than a hash
6 value for a file, correct?

7 A. It is certainly different.

8 Q. So the info hash is just saying, hey, I've got this
9 information and you want it or vice versa, and we're going to
03:54 10 now have this handshake and hookup, right?

11 A. Well, it's more specific than a file hash. I just want to
12 be clear. Info hash is different. It's a hash with
13 information. But the information in hashes are the file names,
14 the file sizes, the SHA-1 hash of every piece. So indirectly
03:58 15 the info hash actually defines the material being traded,
16 whether that be one file or 100 files. So it's better than a
17 file hash.

18 Q. Okay. So that's -- so an info hash is different than a file
19 hash, right?

03:59 20 A. Yes.

21 Q. And then a file hash is different than the file itself,
22 right?

23 A. It's the fingerprint or signature of the data.

24 Q. But it's not the thumb, it's the thumb's fingerprint, right?

03:59 25 So it's not the same thing.

1 A. (No audible response.)

2 Q. So, in other words, if you can get a file hash, does that
3 give you the file?

4 A. No. The file hashing is a unidirectional thing.

04:00 5 Q. It's an algorithm, right?

6 A. Right.

7 Q. It's a 40-digit hexadecimal whatever, it's not the file
8 itself, correct?

9 A. Correct.

04:00 10 Q. Okay.

11 A. The hash points to the file.

12 Q. Now, I think you testified earlier and correct me if I'm
13 wrong, the name of the file is inside the torrent, right?

14 A. Yes. And the [Indiscernible].

04:02 15 Q. Okay. And so, for example, like on Exhibit I believe it
16 was -- let me just make sure I'm getting this one right.

17 So on Exhibit 5 I believe, where it says "torrent file
18 fragments," right?

19 A. Yeah.

04:02 20 Q. And it has the -- you know, the name right there under the
21 name column.

22 A. Yes.

23 Q. Starting, you know, "022Asian," okay?

24 A. Yes.

04:02 25 Q. And then in the source column it's got the hash file

1 torrent, right?

2 A. It's -- basically what it's done is it's named the torrent
3 by its info hash.

4 Q. Right. So that name is inside, like you said, the hash.

04:03 5 It's part of the information that's in the hash file.

6 A. It's part of the information in the hash, so, yes.

7 Q. But again, that's not the file itself.

8 A. That is not the file --

9 Q. And you don't contest again that the file that supposedly
04:03 10 was downloaded here two days in a row wasn't recovered later,
11 right?

12 A. I don't contest that. Although the other exhibit shows it
13 was there, the MRU. That's the file, that's not the torrent.

14 Most recently used, which was Exhibit 6, show you that
04:03 15 file name including its extension. That's when you open the
16 file in a video player, for instance. And that was on May 22nd,
17 after the first investigation and just before the second
18 investigation. MRU is the file.

19 Q. Yeah. Gotcha. Now, you talked about false positives. You
04:04 20 would agree that just because a false positive might be rare,
21 it's not impossible, right?

22 A. Well, statistically speaking it's 1 and 1.4 quindecillion
23 or two to the 160th power.

24 Q. That's of two hash values not matching, that's not the same
04:06 25 thing as whether or not there might be a false positive in a

1 software, which is a type of malfunction or bug in the software,
2 correct?

3 A. Right.

4 Q. So I'm not asking the odds of two hash values matching,
04:07 5 which I understand is an impossibly high number, I'm saying that
6 just because a false positive might be rare within this program
7 that we don't have access to, doesn't mean it's impossible.

8 A. (No audible response.)

9 Q. And I can --

04:07 10 A. There's so many areas a false positive could be, you'd need
11 to define that further. Because the data we receive as hashed,
12 it's impossible -- or at least two to the 160th power that that
13 is not the data that belongs to the torrent.

14 Q. Let me put it -- can I put it this way? Okay. So you have
04:08 15 these hash values which are indicators of the file on the
16 computer, right?

17 A. Are we -- the info hash of a torrent, is that what we're
18 talking about?

19 Q. Or the torrent. The torrent is not the file itself, it's an
04:08 20 indicator of the file, right?

21 A. It's the instructions to download file.

22 Q. Okay. And we also have like this, you know, again most
23 recently used whatever with, you know, the extension, right?
24 But again, it's not the file itself.

04:09 25 A. That's the file itself was touched which caused an entry,

1 MRU entry.

2 Q. But an MRU entry is not the file.

3 A. No, no, no, you're right.

4 Q. Okay.

04:09 5 A. It's just proof that the file was there.

6 Q. And you've speculated that the reason the file isn't there
7 and only these indicators are there is because perhaps it was
8 deleted, right?

9 A. Correct.

04:10 10 Q. And that's possible. It's also possible it was a false
11 positive; that the program reported the file as being there and
12 it really wasn't. I'm not asking again about hash matches or --
13 I'm saying is that possible?

14 A. It's not possible because the detailed log -- there's no way
04:11 15 he could have sent us 226 pieces with the corresponding hash
16 values unless it was present at that moment in time on his
17 computer. So this, I say, no, it's impossible.

18 Q. I'd like to ask you a hypothetical. Okay? Let's say the
19 Torrential Downpour Receptor, just like every other computer
04:12 20 program, whether it's Windows, Microsoft Excel, you name it,
21 whatever, has a bug in it. And I understand you said there was
22 only one. Let's say it has a bug in it, okay? And it's not
23 performing properly. Those log files are generated from the
24 program, correct?

04:12 25 A. Correct.

1 Q. So if there was a problem with the program there could also
2 be a problem with those log files.

3 A. I don't -- I agree that if there's a problem with the
4 program it could affect the log file. But what it couldn't do
04:12 5 is make 226 pieces match. There's no possibility that the
6 computer at that IP address didn't possess that whole file
7 because he shared 226 matching pieces. It's not a possibility.

8 Q. But the log files which says it matched 226 pieces, fair?

9 A. It is what it says, yes.

04:16 10 Q. Okay.

11 A. And so we would have had to get wrong and have it match 226
12 times. It's just inconceivable to me. I don't know how to
13 better answer your question. I apologize.

14 Q. I guess my final question would be: So a false positive is
04:17 15 possible.

16 A. Anything's possible. But statistically speaking, I don't
17 believe it happened here.

18 Q. I understand.

19 MR. DONOVAN: I don't have any other questions,
04:17 20 Your Honor.

21 THE COURT: All right. Thank you, Mr. Erdely.

22 THE DEFENDANT: Thank you, Your Honor.

23 (Witness excused at 4:42 p.m.)

24 THE COURT: Mr. Donovan, what would you like to do?

04:20 25 MR. DONOVAN: Well, Your Honor, I'm kinda torn.

1 Obviously I think this is complicated stuff. I think we've
2 learned a lot today. I know my expert whispered to me that he's
3 learned a lot today. So I think we might have some of our
4 questions answered, but not all of them.

04:20 5 THE COURT: I'm -- you know, when you have an expert
6 like Mr. Erdely come in, I don't get this stuff much, I don't
7 think the government wants to produce him over and over and
8 over, so it probably makes sense for me to write something. And
9 if I'm going to write something on this, I think you should tell
04:21 10 me what you -- your position after hearing the evidence.

11 MR. DONOVAN: Well, and that's what I was getting
12 towards, is I'm -- I think I'm leaning towards I'd like to get
13 the transcripts, have some time to review those, I guess do a
14 follow-up, you know, brief or, you know, position.

04:22 15 THE COURT: Transcripts? Can't you give me something
16 faster? I mean, this case has been --

17 MR. DONOVAN: I know.

18 THE COURT: This is an 18 -- when was this filed, back
19 in July of last year? And there were a lot of delays in getting
04:22 20 you as much as we did get. Then you got an expert.

21 MR. DONOVAN: I understand, Your Honor. And I do
22 appreciate the Court's patience with this case because, again,
23 at least from my perspective, this has been complicated and
24 difficult to work through even with the expert because, again,
04:23 25 we have an asymmetry of information here trying to figure out

1 what's going on.

2 THE COURT: What makes this case unique? I mean, we
3 have all these child pornography cases. Is it just that he's
4 charged with distribution and the files he was charged with
04:23 5 distributing weren't found on the -- the files themselves were
6 no longer -- or not found on his computer?

7 MR. DONOVAN: I think that's exactly right. I think
8 what the big difference we have here is that they're pretty
9 convinced that it must be because it was deleted. Okay?

04:24 10 We're --

11 THE COURT: There were a lot of files that were on the
12 computer, correct? I mean, there's possession charges here.

13 MR. DONOVAN: Yes, later. Yes. Count 2 relates to
14 the search warrant and the stuff that came from the search
04:26 15 warrant. That's a simple possession charge. Has no mandatory
16 minimum.

17 Count 1 relates only to these two downloads from
18 Torrential Downpour Receptor. And that's what was not located
19 on the media. And so --

04:27 20 THE COURT: Did you know that there was -- 4, 5 and 6
21 showed that it was on the -- or at least there's pretty good
22 evidence that --

23 MR. DONOVAN: Well, again, these are artifacts. You
24 know, these are indicators, these aren't the files. I mean,
04:27 25 this is -- this is what I was trying to get on my rebuttal

1 questions there.

2 THE COURT: Yeah.

3 MR. DONOVAN: 4, 5 and 6 show things taken from the
4 system through a -- basically a forensic program, right? And
04:27 5 they're indicators of the file, they're not the file. I don't
6 think it's being disputed here and I think he even admitted
7 on --

8 THE COURT: So I guess my question is: Is this more a
9 question of the search or are we beyond that now and this is a
04:28 10 question of just your ability to assert your defense and --

11 MR. DONOVAN: I think it's two things. I think, one,
12 it's the ability to properly prepare for trial, should there be
13 a trial here, of the government witness who ran this program and
14 says that these things were downloaded because, again, they're
04:28 15 not later recovered, okay?

16 So the only evidence that the government's going to
17 present about that is what this program did and what it
18 supposedly observed and downloaded and generated logs about and
19 all of that. That's how they're going to prove Count 1.

04:28 20 They're not going to prove Count 1 because it was
21 located later on his computer. Count 1 is a distribution charge
22 that carries a five-year minimum, so that's obviously the one
23 that we're more concerned about.

24 And, I would also mention, Your Honor, what happened
04:29 25 in Count 1 during this program running is the sole basis of the

1 search warrant that is then later used to form the basis of
2 Count 2, to go get the warrant executed, locate whatever they
3 locate and then charge possession.

4 So I think it relates more directly to Count 1, and I
04:30 5 think that's what makes this case more unique than other cases
6 where they do later recover the file or whatever. But it also
7 does impact Count 2. And it impacts it on I think several
8 levels, but definitely preparing for trial and cross-examining
9 the government --

04:30 10 THE COURT: Are you suggesting that the program
11 actually puts child pornography on the defendant's computer?

12 MR. DONOVAN: No. I don't think we have any
13 indication of that. I'm not going to advance that. I asked a
14 couple questions about that.

04:30 15 Again, I think the question for Count 1 is could this
16 be a false positive, which is why it's not there when they go
17 back later to look, versus he deleted it.

18 THE COURT: So even if it's a false positive, let's
19 say, it's still probable cause.

04:31 20 MR. DONOVAN: Yes.

21 THE COURT: So --

22 MR. DONOVAN: So in that case it could still support
23 Count 2. But then it would not support Count 1 because that
24 would mean that it was never there. Count 1 is that he, on a
04:31 25 specific date, distributed this specific file.

1 THE COURT: Well, they'd still get to a jury on
2 Count 1 because they'd certainly be able to argue from the logs
3 and the search of the computer, the mirrored computer, the data
4 they have there; that he actually possessed it, he just deleted
04:31 5 it.

6 MR. DONOVAN: Yes, I think that could get to the jury.
7 That could be arguable. That's where we're handicapped because
8 we don't have access to this program and can't question its
9 reliability, accuracy. I mean, this is the problem.
04:31 10 Everything, with all due respect to the government witness,
11 is --

12 THE COURT: Okay. Let's say it takes a week to get a
13 transcript. When will I see your brief?

14 MR. DONOVAN: Well, Your Honor, I'm on vacation from
04:32 15 August 23rd until September 2nd, so I think that's the day
16 before Labor Day. I mean, I'll do it as fast as I can after
17 that, but my, you know --

18 THE COURT: Okay. So how about September 10th. 15th?

19 MR. DONOVAN: Sure. I'm assuming that the transcript
04:32 20 hopefully comes through.

21 THE COURT: September 15th for your brief, Mr. Humble?

22 MR. HUMBLE: Whatever you'd like, Judge.

23 I'll just say, we were told -- and I know it's on the
24 recordings -- repeatedly when we were having these continued --
04:32 25 what am I -- adjournments to --

1 THE COURT: Status conferences.

2 MR. HUMBLE: Correct. -- that this was dispositive;
3 that there wasn't going to be a trial. I understand --

4 THE COURT: This motion would be dispositive.

04:33 5 MR. HUMBLE: I understand things change.

6 THE COURT: Yeah.

7 MR. HUMBLE: But it was repeatedly asserted by counsel
8 that this was dispositive, that there wasn't going to be a
9 trial, but this was the issue that we were basically going to
04:33 10 battle out. Now that's not what I'm hearing. So....

11 THE COURT: Well, my sense is if he's -- if the
12 motion's denied am I likely to see a -- then it's probably not a
13 trial.

14 MR. DONOVAN: Well, that's exactly what I meant when I
04:33 15 said dispositive before. Obviously if we don't get this, that
16 changes things drastically I think from our perspective and then
17 it probably -- yeah, I don't know at that point how we could
18 effectively even prepare for trial. If it's granted, then that
19 would be a different story because then we could actually maybe
04:34 20 get even further answers than what we've gotten so far.

21 THE COURT: Yeah. 30 days after his. And the sooner
22 the better. And then if you want to reply, 10 days later,
23 Mr. Donovan.

24 MR. DONOVAN: Okay.

04:34 25 THE COURT: And I appreciate this is delayed, but I

1 take it there's been compliance. There's no noncompliance with
2 conditions of bail as with most of these cases?

3 MR. DONOVAN: Correct, he's been --

4 THE COURT: And frankly I -- you know, this is very
04:34 5 unusual. If the government needs to go through this on every
6 child pornography case, that's -- we're going to see far fewer.
7 You can't -- and the government has made the effort of calling
8 an expert who frankly is acknowledged as the expert on this
9 program. So I think since they've made that record I'll try and
04:35 10 give you something that will have some value.

11 MR. DONOVAN: Thank you. I would just note September
12 15th's a Sunday. Can we do September 16th which is Monday?

13 THE COURT: Sure. Any day I selected that is a
14 weekend, take the next day.

04:35 15 MR. DONOVAN: Okay, thank you.

16 THE COURT: All right. Anything else today?

17 MR. HUMBLE: Not from the government.

18 THE COURT: All right. Thank you, all.

19 MR. HUMBLE: Thank you.

04:36 20 UNIDENTIFIED SPEAKER: Thank you, Your Honor.

21 (Hearing adjourned at 4:49:46 p.m.)

22 * * *

23

24

25

C E R T I F I C A T E

I, JOHN T. SCHINDHELM, RMR, CRR, Official Court Reporter and Transcriptionist for the United States District Court for the Eastern District of Wisconsin, do hereby certify that the foregoing pages are a true and accurate transcription of the audio file provided in the aforementioned matter to the best of my skill and ability.

Signed and Certified August 30, 2019.

/s/John T. Schindhelm

John T. Schindhelm

John T. Schindhelm, RPR, RMR, CRR
United States Official Reporter
517 E Wisconsin Ave., Rm 236,
Milwaukee, WI 53202
Website: WWW.JOHNSCHINDHELM.COM



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25

I N D E X

<u>WITNESS</u>	<u>EXAMINATION</u>	<u>PAGE</u>
PEYTON ENGEL, DEFENSE WITNESS		
	DIRECT EXAMINATION BY MR. DONOVAN.....	3
	CROSS-EXAMINATION BY MR. HUMBLE.....	37
	REDIRECT EXAMINATION BY MR. DONOVAN.....	45
ROBERT ERDELY, GOVERNMENT WITNESS		
	DIRECT EXAMINATION BY MR. HUMBLE.....	50
	CROSS-EXAMINATION BY MR. DONOVAN.....	90
	EXAMINATION BY THE COURT.....	114
	FURTHER CROSS-EXAMINATION BY MR. DONOVAN.....	118

E X H I B I T S

<u>NUMBER</u>	<u>DESCRIPTION</u>	<u>OFFERED</u>	<u>ADMITTED</u>
1	Erdely CV.....	50	50
1	CV of Robert Erdely.....	90	90
2	Investigative log for download 5/21/18.....	90	90
3	Investigative log for download 5/22/18.....	90	90
4	Installed Programs.....	90	90
5	Torrent Files.....	90	90
6	MRU Recent Files and Folders.....	90	90